

TECHNICAL DOCUMENT 3182
June 2004

Secure Enterprise Access Control (SEAC) Role Based Access Control (RBAC)

Prepared for
Commander, U.S. Pacific Fleet
SEPM
NAVSTA Building 352
Pearl Harbor, HI 96860



Prepared by
Richard Fernandez
SSC San Diego
675 Lehua Ave, Building 992
Pearl City, HI 96782
(808) 474-9270, fax (808) 471-5837
richard.r.fernandez@navy.mil



The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

Approved for public release:
distribution is unlimited.

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE JUN 2004		2. REPORT TYPE		3. DATES COVERED 00-00-2004 to 00-00-2004	
4. TITLE AND SUBTITLE Secure Enterprise Access Control (SEAC) Role Based Access Control (RBAC)				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) SPAWAR Systems Center,675 Lehua Avenue Building 992,Pearl City,HI,96782				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES The original document contains color images.					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES 84	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

SSC SAN DIEGO
San Diego, California 92152-5001

T. V. Flynn, CAPT, USN
Commanding Officer

R. F. Smith
Executive Director

ADMINISTRATIVE INFORMATION

This paper discusses a government off-the-shelf-solution for Role-Based Access Control (RBAC) proposed by Richard Fernandez, Space and Naval Warfare Systems Center, San Diego (SSC San Diego) for Commander, U.S. Pacific Fleet (COMPACFLT).

Released by
Kent K. Kuriyama, Head
Code 24244, SSC San Diego

Under authority of
G. Fred Kramer, Acting Head
Code 2422, SSC San Diego

Acknowledgements

The author wishes to acknowledge the following individuals: Wilfredo Alvarez, Wallace Fukumae, Ryan Kanno, and Tuan Huynh.

Trademarks

Company names are registered trademarks or trademarks of their respective companies.

Invention Disclosure

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

Resources

TRUSTe Privacy Seal: <http://www.eTrust.com>
National Institute of Standards and Technology, Role Based Access Control:
<http://csrc.nist.gov/rbac/>

Revisions

Initial Publication

1 June 2004 Richard Fernandez

EXECUTIVE SUMMARY

This paper discusses a government off-the-shelf-solution (GOTS) for Role-Based Access Control (RBAC) proposed by Richard Fernandez, Space and Naval Warfare Systems Center, San Diego (SSC San Diego) for Commander, U.S. Pacific Fleet (COMPACFLT).

Problems with access control list (ACL) and security implications. Access to resources such as applications and web services are becoming increasingly difficult to manage via access control lists (ACLs). ACLs usually consist of a client's name or unique identifier. However, resource access is usually based on client characteristics such as command assignments, clearances, and/or pay grade. If a user is reassigned, changes clearance, or is promoted, access to resources should also change. Instead, with ACLs, resource managers constantly have to evaluate personnel records to determine resource access. Such a task can become overwhelming as the number of personnel within an organization grows. Limited access to personnel records by resource managers could compound the problem. In an RBAC solution, a resource manager does not have to constantly query personnel records to determine resource access. The resource manager establishes conditions based on a user's characteristics (command assignments, clearances, and/or pay grade) versus their name or unique identifier.

Another limitation with ACLs is the existence of security conditions. Homeland Security and regional Information Assurance agencies are authorized to impose security threat levels that may affect access to a wide range of resources by many personnel. Sudden changes in security conditions may not allow sufficient time to modify an ACL, thereby creating possible security breaches by unauthorized personnel. Finer granularity of resource access may be required during certain security conditions. For example, during Information Conditions (INFOCONs) C and D, only "administrator" and "superuser" account holders would be granted access, while all "guest" and "user" accounts would be denied access. An RBAC solution can accommodate these kinds of scenarios by pre-configuring resource access for all INFOCONs. Once an INFOCON state changes, the RBAC would only evaluate the conditions already established for the prevailing INFOCON.

Introducing an effective RBAC. Because of ACL limitations, the National Institute of Standards and Technology (NIST) has mandated RBAC as the compliance mechanism for granting resource access. RBAC offers an automated process to manage resource access based on a user's role. Therefore, any role change effectively affects resource access. The definition of a role can be a title/position designation within an organization. In this RBAC proposal, a role consists of many attributes such as branch of service, billet title, pay grade, clearance, attached organization, etc. These user profile attributes are compared with the conditions established by the resource manager to determine resource access. For example, a resource manager establishes a set of conditions (referred to as a resource profile) for accessing a Project Tracker application. The following resource profile lists three conditions that will allow "administrator" access to Project Tracker:

- E4 & above,
- Top Secret clearance,
- NavMagHawaii assignment

A user's profile will have to match the above three conditions in order to gain access to the Project Tracker application as an administrative user.

How the RBAC would work. Personnel data would be queried (on a real-time basis from authoritative data sources), compiled into one or more user profiles, presented to a client for

profile selection, and submitted to the RBAC. The RBAC would then return a list of accessible resources based on the user profile. The client would then select a specific resource, and the RBAC will again process the user profile but present a list of resource role(s) (or accounts such as “guest” or “administrator”) for selection. The client would then select a specific resource role, and an access token would be issued to the resource for access.

User profiles. A user profile should consist of a unique set of attributes that identifies the client. Attribute values should be assigned to a corresponding profile. A client should never be allowed to switch attribute values among user profiles in order to gain access to a resource. Here is an example:

<u>Categories</u>	<u>COMPACFLT Profile</u>	<u>SPAWAR Profile</u>
Organization:	N65	2424
Clearance:	Secret	Top Secret
Paygrade:	DP3	DP3
Service:	DoD	DoD
Function:	Program Manager	Developer

Personnel information should be acquired from an authoritative source and allow users to select a profile.

Customer meta-database. A Lightweight Directory Access Protocol (LDAP version 3)-compliant directory service will be required to store hierarchal information about a command structure, pay grade scales, geographic, job descriptions, clearance levels, etc. The layout of this data could be in a tree structure (i.e., command structure) or in a list (i.e., list of job descriptions). This data structure would serve as a reference to establish conditions to access resources. For example, if a resource manager sets N6 and below as a condition, the RBAC Rules Engine could compare the hierarchal precedence between user and resource profile by comparing their distinguished name formats. Management of these directory services would be delegated to a customer or enterprise entity.

Resource managers (RMs). A RM is assigned the responsibility to establish resource permissions. Commands would have a choice to centrally manage resources or delegate them to subordinate commands. An effective RM would understand the requirements of users before establishing resource condition(s). A web-based resource management interface would allow a RM remote establish permissions.

RBAC integration. Any RBAC solution (commercial off-the-shelf (COTS) or GOTS) will require some level of integration with a customer’s portal and resources (i.e., software applications, web services, etc.). The SEAC RBAC design requires an additional customer furnished and maintained asset called the customer meta-database. This customer meta-database is critical for establishing conditions to access resources. The SEAC RBAC is designed to access an unlimited number of customer meta-databases with a simple tie-in.

RBAC interoperability. The existence of local and regional customer meta-databases offers the RM the capability to establish conditions for local and remote users. A remote user will be allowed access to local resources if a RM has established conditions from corresponding remote customer meta-database(s).

CONTENTS

EXECUTIVE SUMMARY	i
CHAPTER 1 ROLE BASED ACCESS CONTROL (RBAC).....	1
General	1
How Access Control Lists (ACLs) Work.....	1
How Groups Work.....	2
How RBAC Works.....	2
Roles and Users.....	2
Role Hierarchies.....	3
Roles and Operations.....	3
CHAPTER 2 PRODUCT OVERVIEW	4
What Is the SEAC RBAC?	4
Essential Criteria for Resource Access.....	4
Why is the SEAC RBAC Unique?	5
Why is the SEAC RBAC Necessary?	5
Customer Cost Savings.....	5
Security	5
RBAC Compliance Is a Federal Requirement.....	5
How the SEAC RBAC Would Work	6
SEAC RBAC Implementation.....	9
RBAC Algorithms	11
Resource Managers (RMs).....	12
SEAC RBAC Interoperability.....	12
Overview of Product Features	14
Resource Pane	14
Resource Role Pane	14
Resource Profile Pane	15
SEAC RBAC Patented Features.....	15
Resource Profiles.....	15
Reference Directory Standard and Tie-in.....	16
Security Levels.....	16
Time Constraints	16
SEAC RBAC a Standard Model.....	16
Problems with Standardless RBAC Systems	16
Standard RBAC Approach	16
CHAPTER 3 DIRECTORY SERVICES	17
Directory Services.....	17
Resource Directory.....	17
Reference Directory	17
Managing Reference Directories	19
Creating and Accessing New Reference Directories	19
Editing Reference Directory Data.....	19
Reference Directory Creation Guidelines	19
CHAPTER 4 USER PROFILES.....	21
General	21
Conditioning User Profiles.....	21
CHAPTER 5 RESOURCE ROLES.....	23

General	23
Anonymous Access	23
Role Levels	24
CHAPTER 6 RESOURCE PROFILES	25
Resource Profile Overview	25
What are Resource Profiles?	25
What is the Minimum Requirement to Gain Access?	25
In What Order are Resource Profiles Evaluated?	25
How Do Time Constraints Affect Resource Profiles?	25
Do Conditions Have a Hierarchal Structure?	26
Resource Profile Construct	26
Resource Profile Evaluation Logic	27
Allow and Deny Resource Profiles.....	30
Allow Resource Profiles	30
Deny Resource Profiles.....	31
Resource Profile Selection Types	31
Deprecated Conditions	35
Global Conditions.....	36
CHAPTER 7 TIME CONSTRAINTS	38
Time Constraint Overview.....	38
CHAPTER 8 SECURITY LEVELS	40
General	40
INFOCON Aware Selection	42
INFOCON Aware Unselection	42
Case Studies.....	42
Case Study:.....	42
During INFOCON A:.....	42
During INFOCON B:.....	42
During INFOCON C:.....	43
During INFOCON D:.....	43

Chapter 1

Chapter 1 Role Based Access Control (RBAC)

General

Designed for Commander, U.S. Pacific Fleet (COMPACFLT), the Secured Enterprise Access Control (SEAC) RBAC is a government off-the-shelf (GOTS) solution. The SEAC RBAC design surpasses the NIST RBAC standard requirements and can be used by any U.S. Government organization. Chapter 1 provides the reader with a general background on RBAC and other access control solutions. Chapter 2 provides a product overview of the SEAC RBAC model. Chapters 3 through 8 cover the SEAC RBAC architecture and salient features.

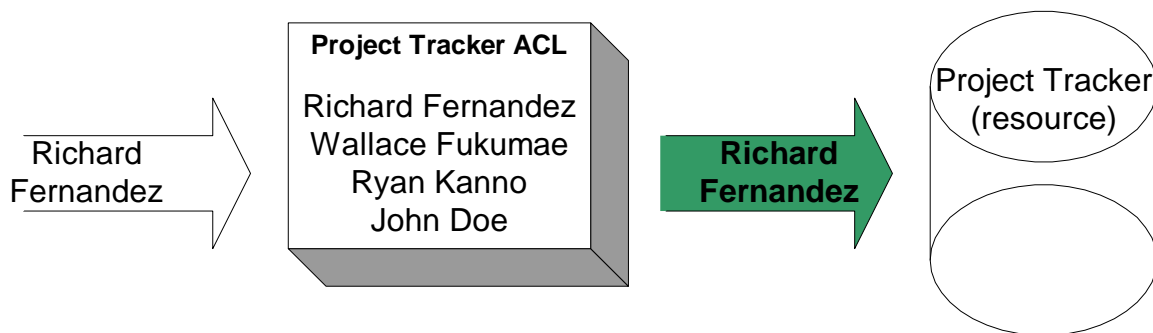
A SEAC RBAC demonstration software application is available for evaluation and training purposes. Permission from COMPACFLT may be required to release the SEAC RBAC demonstration. Please contact Richard Fernandez regarding any comments or suggestions at:

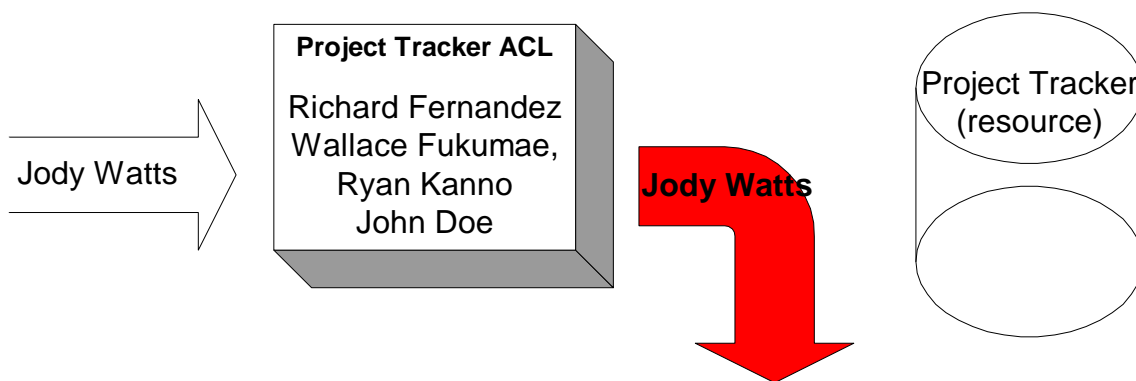
richard.r.fernandez@navy.mil
(808) 478-4937

It is recommended that this document be printed in color.

How Access Control Lists (ACLs) Work

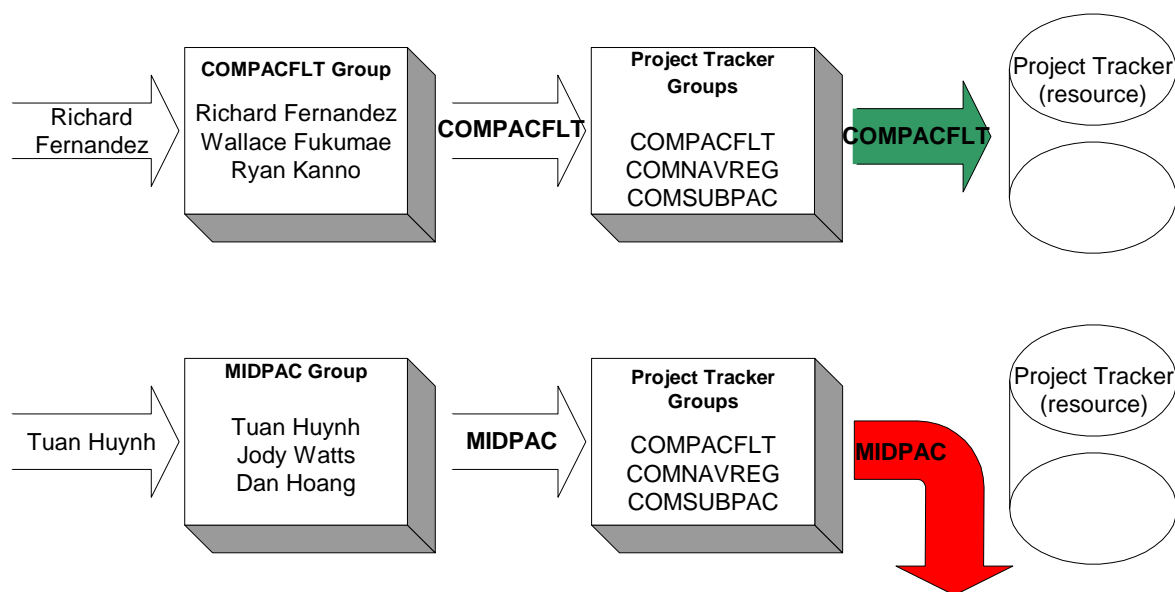
The following diagrams illustrate how an ACL compares names to a list to determine resource access:





How Groups Work

Another way resource access can be determined is by using group association. Unlike ACLs, groups offer a common classification for a list of users. The entire group is then evaluated to determine resource access. The diagrams below illustrate the concept:



How RBAC Works

According to the National Institute of Standards and Technology (NIST) RBAC standard, resource access is determined on roles that individual users have as part of an organization. This method is similar to group association, but the RBAC standard requires that roles be capable of inheritance.

The following sections summarize the NIST RBAC compliance requirements. Note: Italicized material below is quoted from NIST/Information Technology Laboratory (ITL) Bulletin, December 1995. For more information, visit: <http://csrc.nist.gov/rbac/NIST-ITL-RBAC-bulletin.html>

Roles and Users

"With role-based access control, access decisions are based on the roles that individual users have as part of an organization. Users take on assigned roles (such as doctor, nurse, teller, manager). The process of defining roles should be based on a thorough analysis of how an

organization operates and should include input from a wide spectrum of users in an organization.

"Access rights are grouped by role name, and the use of resources is restricted to individuals authorized to assume the associated role. For example, within a hospital system the role of doctor can include operations to perform diagnosis, prescribe medication, and order laboratory tests; and the role of researcher can be limited to gathering anonymous clinical information for studies.

"The use of roles to control access can be an effective means for developing and enforcing enterprise-specific security policies, and for streamlining the security management process."

Role Hierarchies

"Under RBAC, roles can have overlapping responsibilities and privileges; that is, users belonging to different roles may need to perform common operations.

"In the healthcare situation, a role Specialist could contain the roles of Doctor and Intern. This means that members of the role Specialist are implicitly associated with the operations associated with the roles Doctor and Intern without the administrator having to explicitly list the Doctor and Intern operations."

Roles and Operations

"Organizations can establish the rules for the association of operations with roles. For example, a healthcare provider may decide that the role of clinician must be constrained to post only the results of certain tests but not to distribute them where routing and human errors could violate a patient's right to privacy. Operations can also be specified in a manner that can be used in the demonstration and enforcement of laws or regulations. For example, a pharmacist can be provided with operations to dispense, but not to prescribe, medication."

Chapter 2

Chapter 2 Product Overview

What Is the SEAC RBAC?

The SEAC RBAC was designed and developed at COMPACFLT during 2003 and 2004. COMPACFLT plans to pilot the SEAC RBAC to access applications within the Secured Enterprise Access Tool (SEAT) framework. The SEAC RBAC system can be used to access any type of resource, with some level of customer integration. Unlike a commercial-off-the-shelf (COTS) RBAC, this GOTS RBAC satisfies unique customer requirements.

Essential Criteria for Resource Access

The necessary criteria for truly determining resource access are user characteristics. Examples of user characteristics are:

- What organization does the user work for?
- What security clearance does the user possess?
- What branch of service is the user under?
- What paygrade category is the user in?
- What job title is user assigned?

Resource access should be affected if a user were to be promoted, change organization, or lose their security clearance. Unfortunately, the methods disclosed in chapter 1 fail to fully consider various user characteristics as the criteria for determining resource access.

The figure below compares how the various access control mechanisms evaluate user characteristics:

	User Characteristics	
	Number of user characteristics evaluated	Hierarchal evaluation of user characteristics
ACLs	0	No
Groups	1	Yes & No
NIST RBAC	1	Yes
SEAC RBAC	Unlimited	Yes

Why is the SEAC RBAC Unique?

The SEAC evaluates an unlimited number of user characteristics (or user profiles) to determine resource access. Therefore, any changes to a user profile or customer organization structure, salaries, job titles, etc. (customer meta-database) could affect resource access.

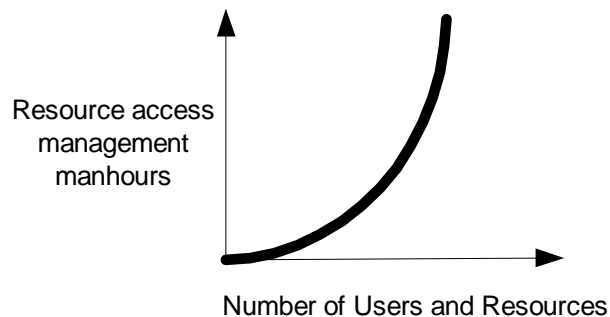
Why is the SEAC RBAC Necessary?

The SEAC RBAC can offer any organization the following benefits:

- Cost savings
- Security
- Compliance

Customer Cost Savings

Because ACLs and groups do not have an automated process to evaluate user profiles, many manhours are required to review personnel records to ensure users should still belong in ACLs or groups. The number of resource management manhours would increase as users and resources increase.



Security

Single sign-on. Access to an RBAC system requires a single sign-on, therefore alleviating users from managing multiple credentials (logins and passwords) to access different resources. Mismanagement of user credentials could result in security breaches and lost efficiency.

Security levels. The SEAC RBAC is capable of evaluating a different set of pre-configured conditions based on different security levels. For example, once an INFOCON state changes, the RBAC evaluates only pre-configured conditions for that prevailing INFOCON.

RBAC Compliance Is a Federal Requirement

Another reason RBAC requires implementation is that the [National Institute of Standards and Technology \(NIST\)](#) has declared RBAC an American National Standard – ANSI INCITS 359-2004 (approved 19 February 2004). This requires all Federal and military entities to implement RBAC for resource access.

How the SEAC RBAC Would Work

Personnel records that identify a client's pay grade, clearance, organization, etc., are maintained in a customer's authoritative personnel database(s). To interface with an RBAC system user characteristics are queried and compiled into one or more user profiles for user selection. Here is an example of a client with two user profiles:

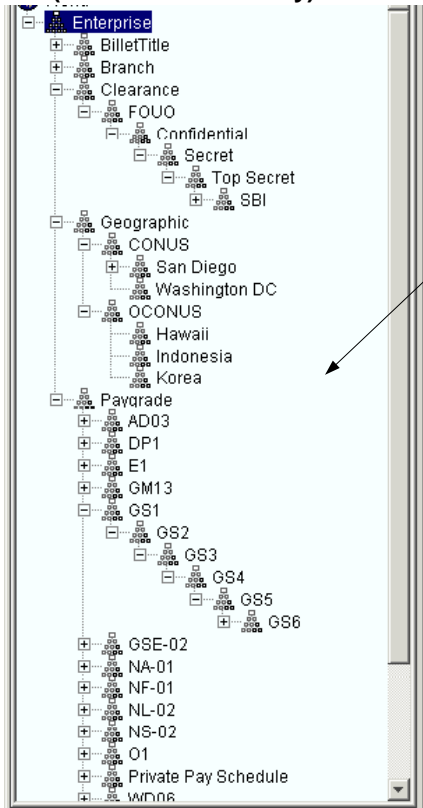
<u>Categories</u>	<u>COMPACFLT Profile</u>	<u>Army Reserve Profile</u>
Organization:	CPF N65	516 th Signal Brigade
Clearance:	Secret	Top Secret
Paygrade:	DP3	02
Service:	DoD	DoAR
Function:	Program Manager	Signal
CPF (COMPACFLT); DP (paygrade designation); DoD (Department of Defense); DoAR (Department of Army Reserves)		

Once a client selects a specific user profile, it is passed to the RBAC Rules Engine for resource access evaluation. The RBAC then returns a list of accessible resources based on the selected user profile. The client then selects a specific resource from a portal, and the RBAC again processes the user's profile and presents a list of accessible resource roles (or accounts such as "guest" or "administrator"). The client can then select a specific role (corresponding to a resource) and finally access the resource.

The following three figures illustrate the general process.

Step 1: A RM assigns a set of conditions to access resources. These conditions are consolidated into resource profile(s).

Customer Meta-Database (Reference Directory)



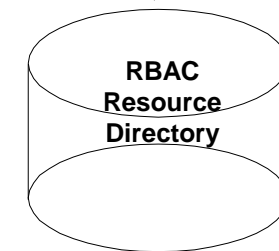
RBAC Condition Manager



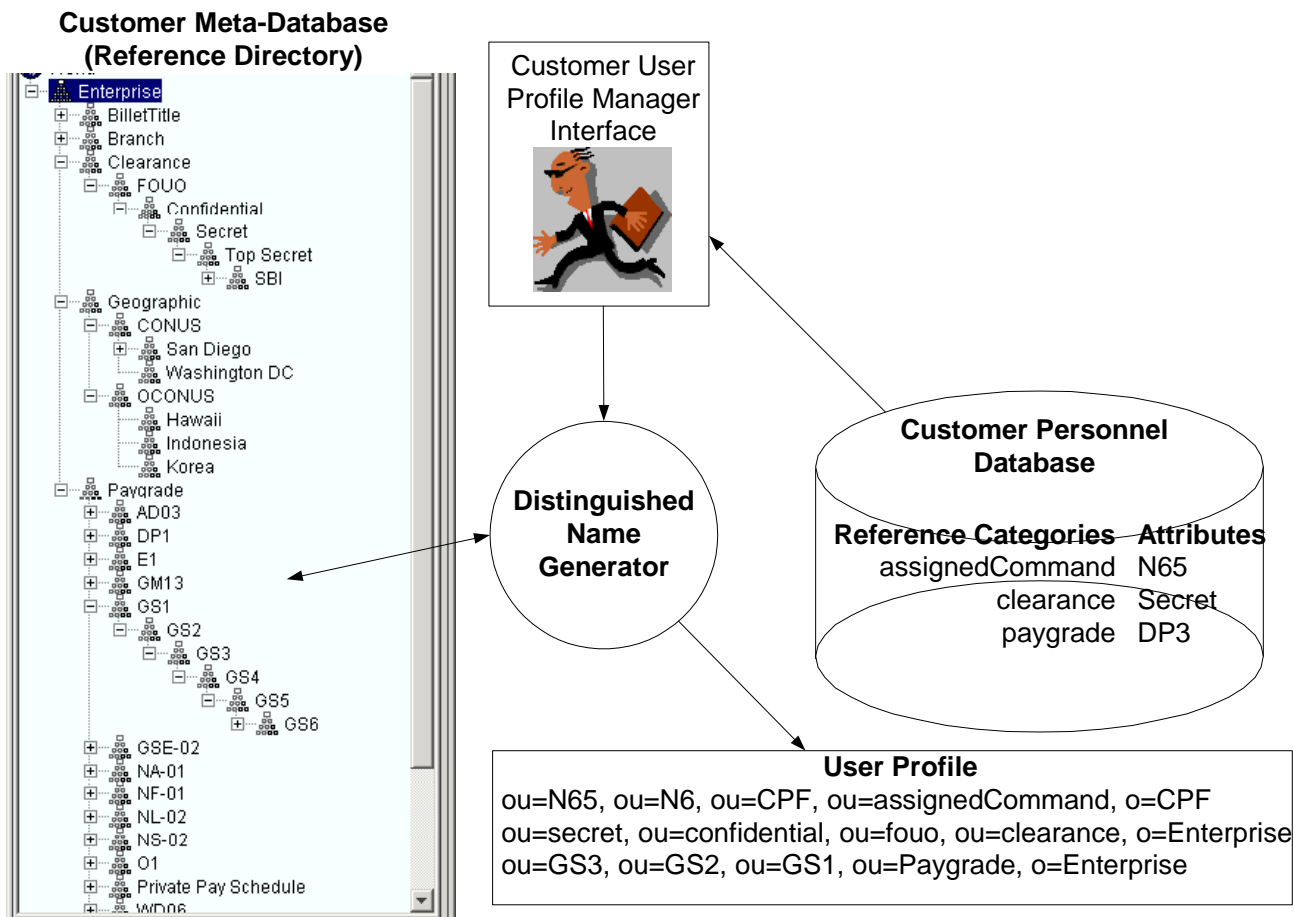
Resource Profile

✓ ou=N65, ou=N6, ou=CPF, ou=assignedCommand, o=CPF
✓ ou=secret, ou=confidential, ou=fouo, ou=clearance, o=Enterprise

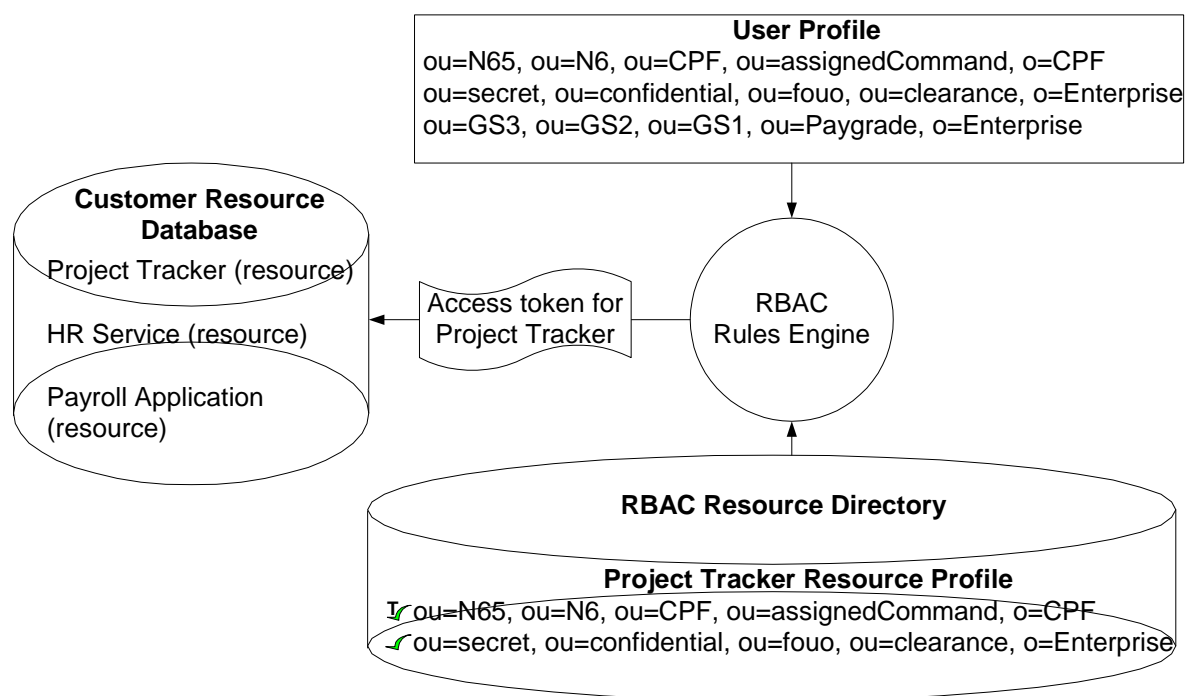
RBAC Resource Directory



Step 2: A client selects a user profile from a customer-furnished user profile manager. The user profile manager queries the customer personnel database for client attributes. These client attributes are then converted into distinguished name format based on the customer meta-database.



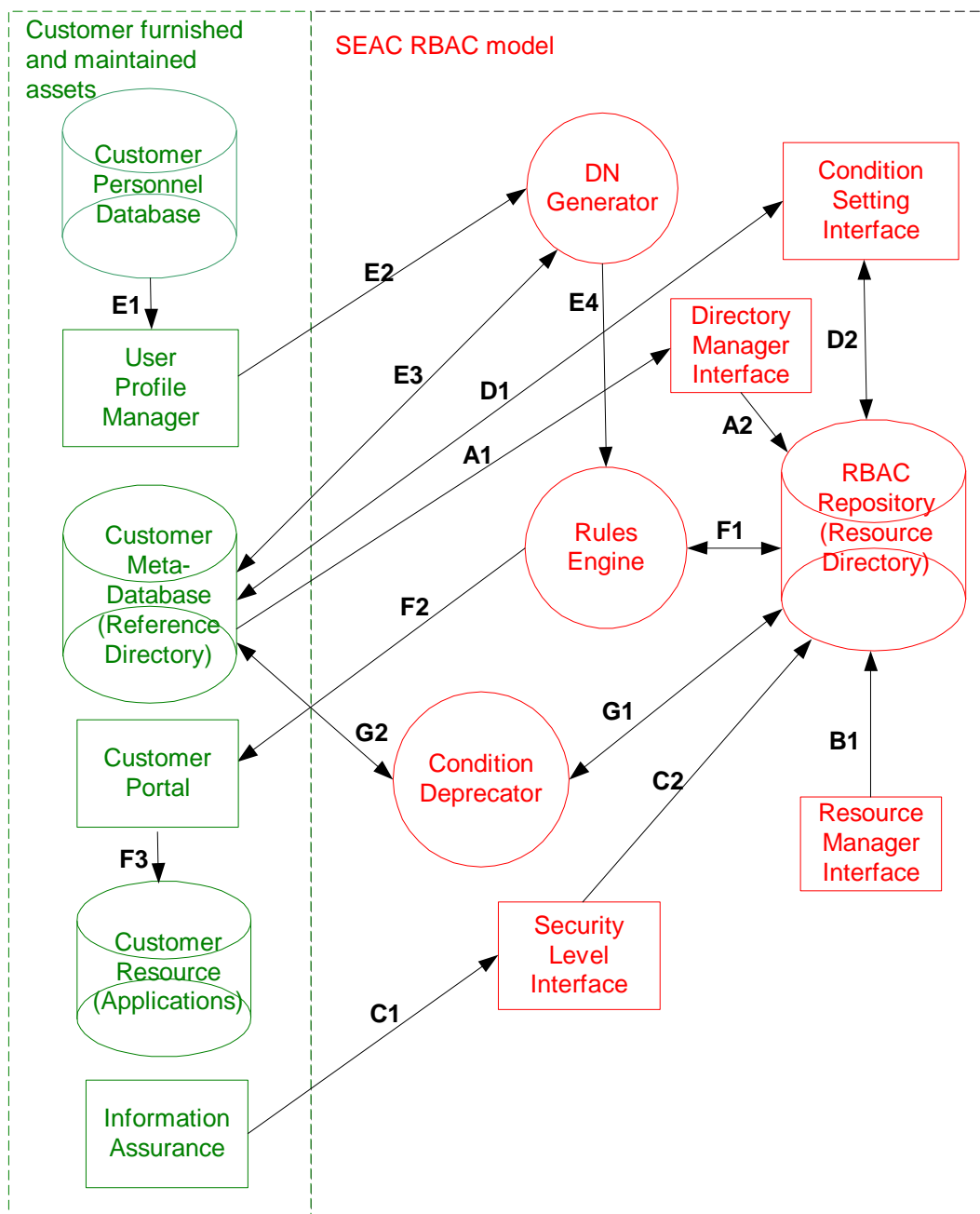
Step 3: The RBAC Rules Engine evaluates user and resource profiles in order to determine resource access.



SEAC RBAC Implementation

This section discusses how the SEAC RBAC would be implemented into a customer's information technology (IT) infrastructure. A list of independent processes is listed below.

- A) Directory Manager Interface – adds, edits, and deletes reference directory referrals.
- B) Resource Manager Interface – adds, edits, and deletes resource repositories for storage of conditions.
- C) Security Level Interface – establishes prevailing Security Levels.
- D) Condition Manager Interface – establishes conditions for access resources.
- E) User Profile Manager – user profile selection and distinguished name (DN) formatting.
- F) Rules Engines – evaluates user and resource profiles to determine resource access.
- G) Condition deprecator – scans reference directory and resource profiles for any changes.



Customer personnel database contains personnel data or characteristic values about the employee, such as their pay grade, job description, and organization assignment.

Customer user profile manager queries the *customer personnel database* in order to present client with a list of user profiles.

Customer meta-database (also referred to as reference directories); the data they contain represent company characteristics such as pay, job description, and organization structures used for establishing conditions for resource access.

Customer portal interfaces with an RBAC to list accessible resources.

Customer resources represents software applications, web services, cipher locks, etc.

Customer information assurance assigns personnel responsible for establishing prevailing security levels (INFOCON, Homeland Security Advisory Level, etc.) so the **Rules Engine** only evaluates pre-configured for resource access.

Condition manager interface is a web interface for resource/security managers to establish conditions to access *customer resources*.

Rules Engine evaluates user and resource profiles (conditions) to determine resource access. The *Rules Engine* consists of a simple string comparison algorithm.

Resource manager interface manages the list of resources and associated conditions in the *resource directory*.

Directory manager interface manages referrals for *customer meta-databases*. Reference directory referrals are stored in the *resource directory*.

Condition deprecator evaluates resource profile conditions with the current state of the *customer meta-database*. Deprecated conditions are flagged in the *condition manager interface*.

RBAC Algorithms

As mentioned above, the current SEAC RBAC model performs simple string comparisons in order to determine resource access. Comparing hash values (versus strings) would improve the performance of the current Rules Engine; however, converting user profiles into hash values on a real-time basis could add even more latency.

There will be requirements to add complex calculations to determine resource access. These complex algorithms would supplement the existing SEAC RBAC Rules Engine. Following is an example of how add-on algorithms would work in conjunction with the SEAC RBAC Rules Engine.

The following user profile is submitted to the SEAC RBAC:

User Profile	
Reference Descriptor	Attribute
Paygrade	GS14
Clearance	Top Secret
AssignedCommand	COMPACFLT N5

The following resource profile would prevent user access because it contains a risk assessment condition that is not contained in the user's profile:

Resource Profile: NavMag Admin	
Reference Categories	Conditions
Paygrade	GS5 and above
Clearance	Secret and above
Risk Assessment	2 and above

Before the user and resource profiles are evaluated by the SEAC RBAC Rules Engine, a risk assessment algorithm could calculate a risk assessment value and append it to the user profile. This risk assessment algorithm may evaluate the current security level and user's clearance to determine the client's prevailing risk assessment as follows:

Clearances	INFOCON A	INFOCON B	INFOCON C	INFOCON D
Confidential	RA2	RA3	RA4	RA5
Secret	RA1	RA2	RA3	RA4
Top Secret	RA1	RA1	RA2	RA3
SBI	RA1	RA1	RA1	RA2

SBI (Special Background Investigation)

If the prevailing INFOCON state were C, the risk assessment algorithm would have calculated a risk assessment value of 2, and it would have been appended to the client's user profile as follows:

User Profile	
Reference Descriptor	Attribute
Paygrade	GS14
Clearance	Top Secret
AssignedCommand	COMPACFLT N5
RiskAssessment	2

The SEAC RBAC Rules Engine would have granted access to this client because the user profile would have matched all the conditions in the resource profile.

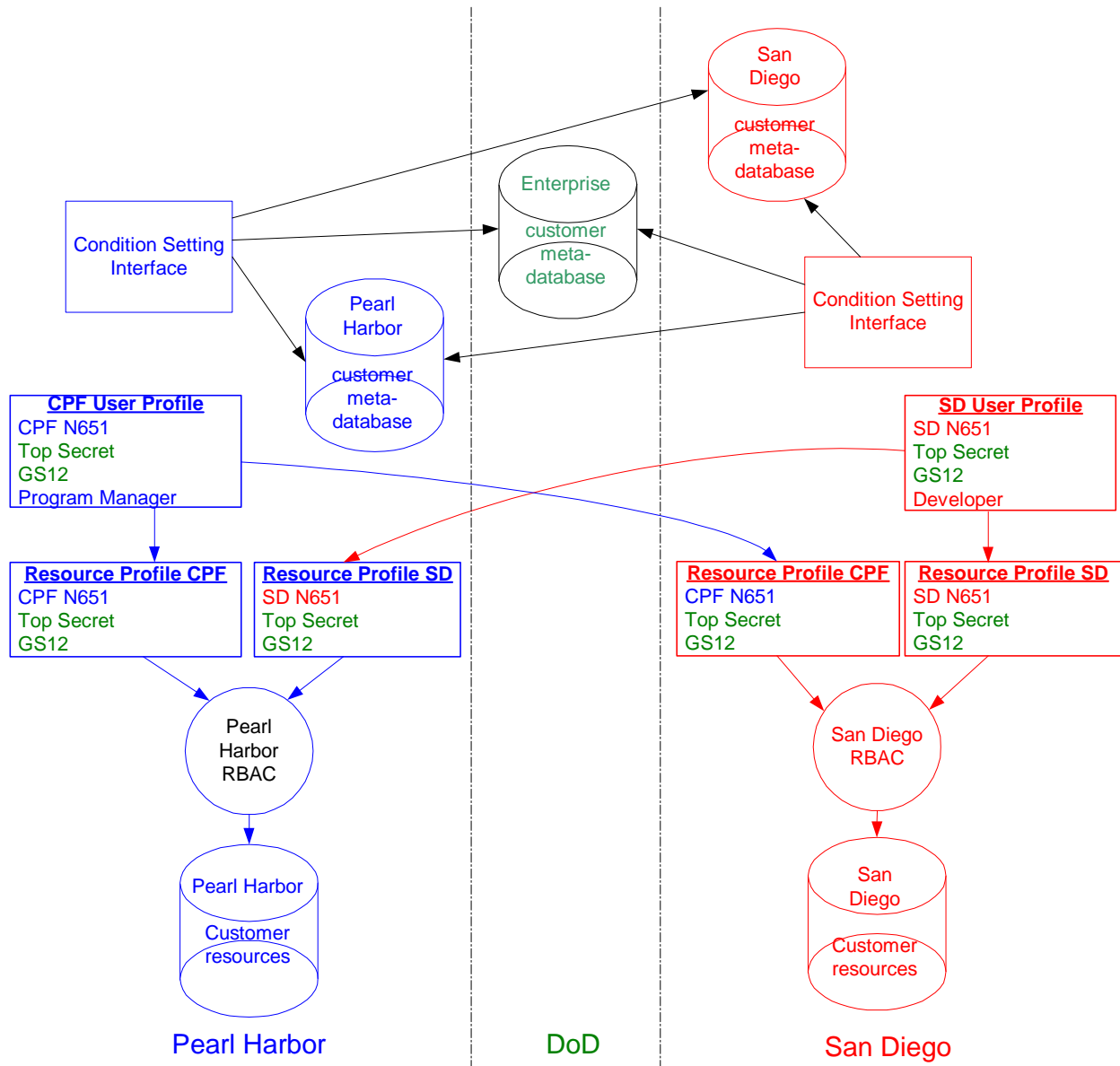
Other types of algorithms would calculate other parameters and append them to the client's user profile for final resource profile evaluation. A standard algorithm tie-in is currently being developed for the SEAC RBAC.

Resource Managers (RMs)

A RM is assigned the responsibility to establish permissions. A command would have a choice to either centrally manage resources or delegate them to subordinate commands. An effective RM has to understand the user requirements before establishing resource conditions. A web-based condition manager interface would allow RMs to establish permissions remotely.

SEAC RBAC Interoperability

The SEAC RBAC framework discussed in this document allows for extension or interoperability among different regions. Dispersed RBAC systems (among regions) are recommended to evaluate access of locally maintained resources. Usually an RBAC system could be co-located at a server farm that processes customer resources such as web services, software applications, etc. Likewise customer meta-databases (reference directories) would be established among local and regional commands. Resource managers from various regions would establish views to these reference directories to establish conditions for remote users. The diagram below illustrates the concept.



San Diego user's can access Pearl Harbor resources because a resource profile was created based on San Diego customer meta-database information. This was easily accomplished because the Pearl Harbor resource manager could view local, regional, and remote reference directory contents via the condition manager interface.

Overview of Product Features

This section outlines the features found in the Resource Management Console (RMC).

Resource Pane

Disabling – prevents access to resource by all users under a respective Enterprise Security Condition.

Enterprise Security Conditions – categorizes resource access conditions based on security threat levels. For example, military applications would use INFOCON A, B, C, D. Government entities would use Homeland Security advisory: Low, Guarded, Elevated, High, Severe. Any organization can incorporate any set of threat levels. An enterprise security condition tie-in will allow the RBAC to evaluate the prevailing security threat.

Notes – notes about this resource can be posted and displayed on a client's portal before and during resource access.

Description – description of this resource can be posted and displayed on a client's portal before and during resource access.

URL – a URL to access information about this resource can be posted and displayed on a client's portal before and during resource access.

Log of user access – furnishes a list of users who have accessed a resource. The log entry contains user unique identifier, resource role (i.e., administrator, user, guest, etc.) and time stamp.

Resource Role Pane

Disabling – prevents access to resource role by all users under a respective Enterprise Security Condition.

Anonymous Access – opposite of disable. This option allows unconditional access to a resource role under a respective Enterprise Security Condition.

Time Constraints – disables the resource role during pre-configured time periods. Time constraints can be set as follows:

Specific time: 1000–1400, Feb 2, 2004.

Recurring weekly: 1730–1800, every Wednesday.

Recurring daily: 1630–1500, everyday.

During resource role time constraints, respective resource profiles (conditions) and associated time constraints are not evaluated.

Role Level – sets up a hierarchy for resource roles. For example, resource roles: **administrator**, **user**, and **guest** accounts (all with the same access conditions) would be assigned role levels 1, 2, and 3, respectively. In this case, the highest resource role level, **administrator**, will be accessible for selection (in customer portal) and not the lower role levels: **user** and **guest**. By default all resource roles are assigned the same role level unless explicitly established by a resource manager. In this case, if the customer had permissions to access **administrator**, **user**, and **guest**, all resource roles would appear on customer portal for selection.

Notes – notes about this resource role can be posted and displayed on a client's portal before and during resource access.

Resource Profile Pane

Disabling – condition is not evaluated by the RBAC.

Allow profiles – condition set that allows access to a resource role.

Deprecated conditions – changes to the customer meta-database affecting resource profile conditions would be flagged.

Allow selection types:

Exact selection – selects a specific condition such as a GS-12 pay grade or Top Secret clearance to access a resource role.

SubTree selection – selects a parent and all associated siblings to access a resource role; for example, GS-5 and above.

Global settings – allow enterprise access on condition.

Deny profiles – conditions that deny access to a resource role. Are evaluated before allow profiles. Deny profiles are used to filter a broad allow condition. For example, an allow condition established for all CPF personnel access could be accompanied with a deny profile that filters or prohibits certain organizations (i.e., N2, N7, and N5) within CPF from access.

Deny selection types:

Exact selection – prohibits a specific condition such as a GS-12 pay grade or Top Secret clearance from accessing a resource role.

SubTree selection – prohibits a parent and all associated siblings from accessing a resource role; for example, GS-5 and above.

Global settings – denies enterprise access on condition.

Time Constraints – disables the resource profile during pre-configured time periods. Time constraints can be set as follows:

Specific time: 1000–1400, Feb 2, 2004.

Recurring weekly: 1730–1800, every Wednesday.

Recurring daily: 1630–1500, everyday.

Notes - notes about this resource role can be posted and displayed on a client's portal before and during resource access.

SEAC RBAC Patented Features

The SEAC RBAC is not only NIST compliant but also features additional patented capabilities:

- Resource profiles
- Reference directory standard and tie-in
- Security levels
- Time constraints

Resource Profiles

According to the NIST RBAC standard, a role can be classified as vocational groups. For example, a role could be a doctor, engineer, or project manager. However, not all organizations, especially the military, can grant resource access based on a job description or duty title. The SEAC RBAC evaluates multiple user characteristics or attributes versus a single attribute such as vocation (or occupation). The SEAC RBAC uses resource profiles to establish conditions to evaluate a user profile. To grant resource access, all resource profile conditions must match a subset of the user profile attributes.

Reference Directory Standard and Tie-in

The SEAC RBAC offers a recommended structure to display and tie-in a customer's meta-database. The reference directories are used in establishing conditions for resource access.

Security Levels

Another unique condition or requirement for accessing resources depends on a prevailing security or threat state. For example, the U.S. military imposes various INFOCON states based on threat levels, i.e., INFOCON A, the most relaxed, and INFOCON D, the most stringent. Facility and resource access change according to prevailing INFOCON states. Other types of Enterprise Security Conditions include Homeland Security advisories. The SEAC RBAC satisfies the evaluation of pre-configured access conditions under various security threats.

Time Constraints

The SEAC RBAC allows automated disabling of resource roles and resource profiles at pre-set time slots. Time constraints can be assigned to resource profiles affecting a specific set of conditions. Time constraints can also be assigned to a resource role globally affecting all assigned resource profiles.

SEAC RBAC a Standard Model

Problems with Standardless RBAC Systems

Existing industry RBAC products currently require a proprietary commitment. A concern with RBAC proprietary solutions is the lack of standard tie-ins with customer assets. A standardless RBAC tie-in with customer assets leaves the customer at a disadvantage because proprietary solutions require some level of customization and maintenance. Customization also leaves the customer at risk if the servicing RBAC vendor can no longer offer support. For example, a manufacturer buy-out could change company policy for supporting an existing RBAC product line and associated customer support. Or a company could cease to exist due to financial reasons. These unforeseen changes could quickly leave a customer's RBAC solution vulnerable. The consequences could be wide-ranging and significant since access control is tightly coupled with security. The only other alternative for the customer is to abandon the existing installed RBAC infrastructure and search for another proprietary RBAC solution. This "fork-lift" approach leaves a customer with financial hardships and disruption of services during RBAC cutovers. For this reason, some customer's have developed an in-house RBAC solution because it assures continued supportability.

Standard RBAC Approach

The [National Institute of Standards and Technology \(NIST\)](#) mandate to adopt an RBAC solution is a step in the right direction. However, the [NIST RBAC standard](#) only offers a theoretical explanation or definition of RBAC. An RBAC integration standard is required to define the tie-ins with customer assets. The SEAC RBAC could represent a NIST-compliant, modular RBAC environment with easy customer integration. Such a standard could offer interchangeable RBAC solutions to seamlessly interface with customer assets. This approach would void the costs of custom coding interfaces and offer long-term support.

Chapter 3

Chapter 3 Directory Services

Directory Services

The SEAC RBAC interfaces with directory services to store and reference information. The protocol used to communicate with these directory services is Lightweight Directory Access Protocol (LDAP) version 3.

There are two types of directory services:

- Resource directories
- Reference directories

Resource Directory

Each region can be designated a single resource directory. This resource directory will be the repository of all resource profiles (or conditions) to access resources. The RBAC Resource Management Console (RMC) (referred to as the Condition Manager Interface) uses the resource directory as a repository of resource profiles. The Rules Engine (RE) queries these resource profiles to determine resource access.

In the RBAC demo the o=SEAC is the designated resource directory. The resource directory contains a list of various resources (i.e., software applications or web services) with their associated conditions for access. The resource directory also contains a referral list of reference directories. This referral list contains LDAP and Transmission Control Protocol/Internet Protocol (TCP/IP) parameters for each reference directory.

Reference Directory

The reference directory contains customer meta-data such as organization structure, employee pay grades, security clearances, job descriptions, etc. Placing the customer meta-database into reference directories has the following advantages:

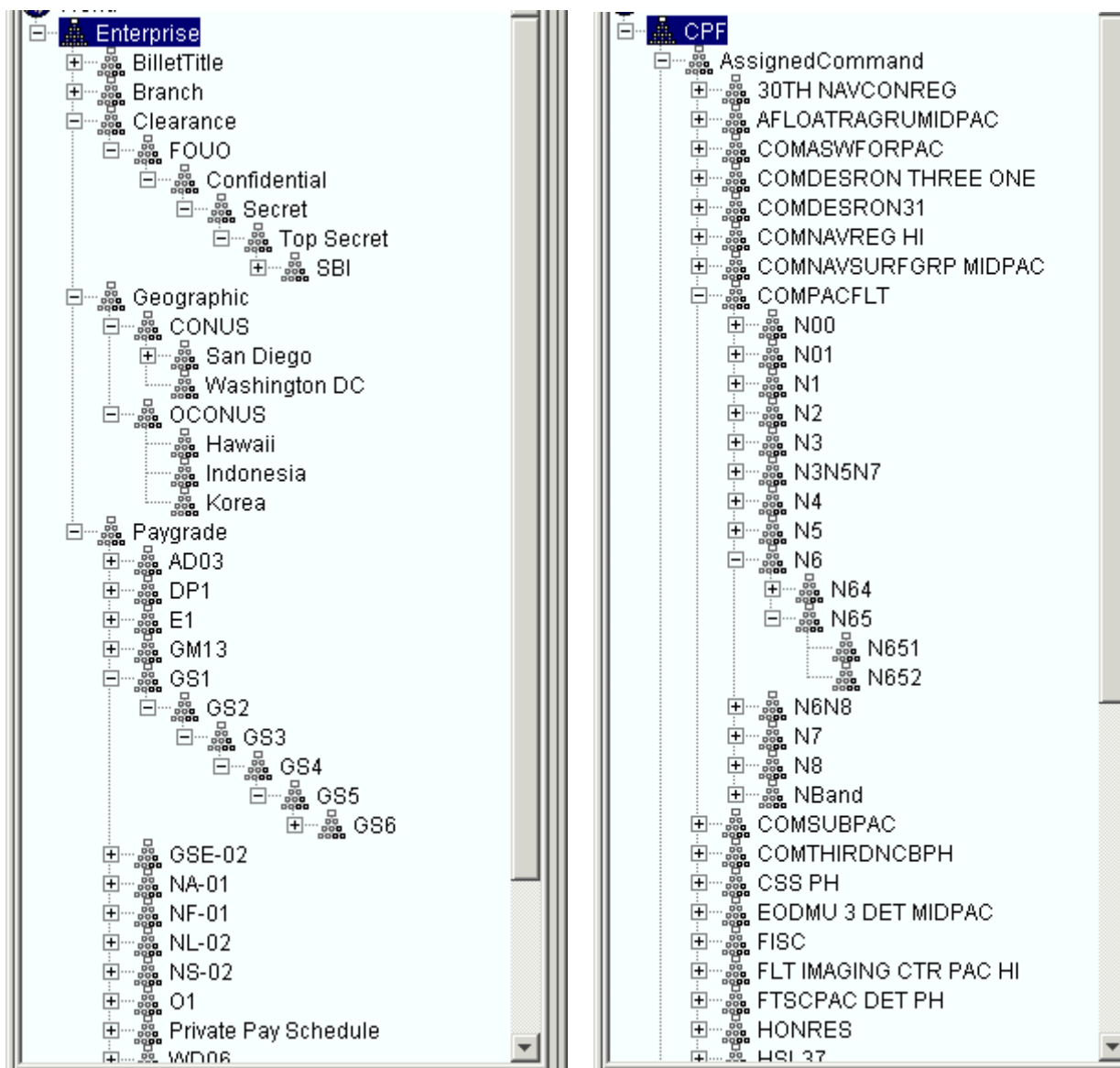
- Furnish benchmarks for inheritance of conditions.
- Maintain a consistent and current status.
- Centralized for ease of management.

RMs are tasked with establishing resource profiles to access resources. The mechanism for establishing these conditions involves selection of values from a series of reference directory services. The contents in these directories correspond to the user profile attributes. These directories furnish RMs with a synchronized and centrally managed customer meta-database. Because this data has to be laid out in a hierarchal format for inheritance purposes, a directory service (versus a relational database) is selected as the platform to store the customer meta-data.

This information can be contained among various directories. Reference directories can be locally or regionally managed. The RBAC demonstration contains two reference directories:

- o=CPF
- o=Enterprise

o=CPF and o=Enterprise represent locally and regionally managed directory services, respectively. The Resource Management Console accesses the reference directories in order to establish conditions for resource access. The figure below illustrates an example of two reference directory contents.



Managing Reference Directories

Unlike the resource directory, reference directories are customer furnished and maintained. However, in order to interface with this RBAC system, the reference directory must comply with simple guidelines. The number of reference directories will depend on customer requirements. If additional criteria data are necessary for establishing conditions, more customer meta-data can be added to existing reference directories. Since information on these reference directories are maintained by an organization, permission will be required to post additional reference categories along with its associated values.

Usually a command or organization will stand up a reference directory of its own that includes cognizant organization structure and other unique attributes not found in other regional reference directories. Before any reference directory is stood up, it is recommended that data contents of other reference directories first be reviewed. Regional or local reference directories could already host information found among various commands or organizations.

Creating and Accessing New Reference Directories

One of the SEAC RBAC's patented features is the ability for easy access to an unlimited number of reference directories. Once a reference directory is established, it can easily be linked to the SEAC RBAC as a referral in the resource directory (not to be confused with reference directory). The Directory Manager tab in the SEAC RBAC Rules Engine demonstration can be used to remotely add, edit, or delete reference directory connection parameters.

Editing Reference Directory Data

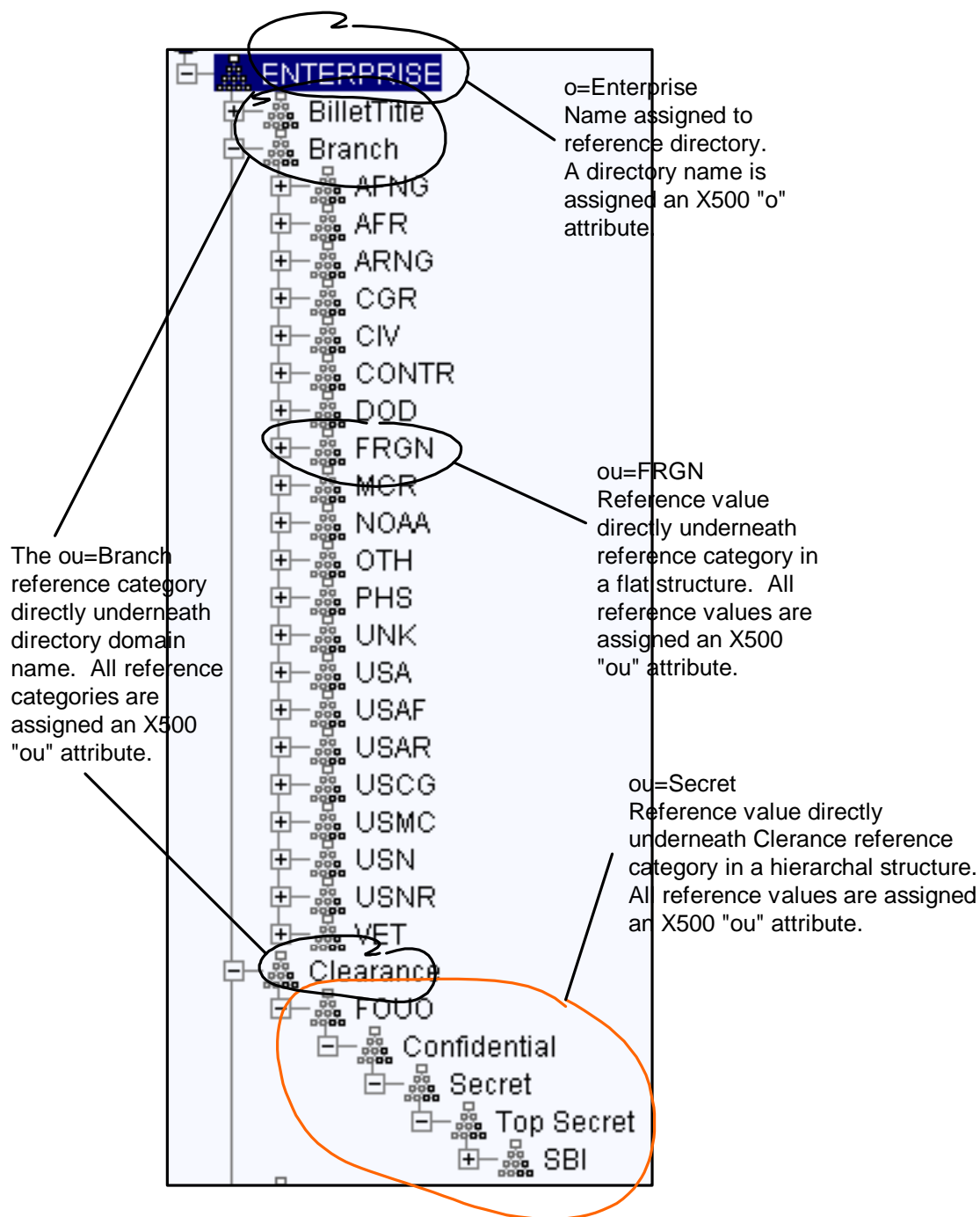
It is recommended that standard operating procedures be established for editing or adding values within the directory. For example, rewriting an organization structure on a reference directory could have drastic effects on existing resource profiles containing old (or deleted) organizational structural conditions. However, expanding an existing organization structure will have no impact on existing resource profiles. A deprecation condition feature on the RMC notifies the RM of any customer meta-database changes affecting existing conditions.

Reference Directory Creation Guidelines

For a reference directory to tie-in with the SEAC RBAC, the following specifications are required:

- 1) Directory must be LDAP v3 compliant.
- 2) There must be network accessibility between Resource Management Console (RMC) and Reference directory.
- 3) The directory domain name value must be assigned to an X500 "organization" class.
- 4) Reference categories must fall under a flat structure directly underneath the directory domain name. All reference categories must be assigned an X500 "organizationalUnit" class.
- 5) The values assigned under a reference descriptor can be flat or hierarchal. All values must be assigned an X500 "organizationalUnit" class.

The following diagram illustrates these requirements.



Chapter 4

Chapter 4 User Profiles

General

The definition of a role can be a title/position designation within an organization. In this RBAC demonstration, a role consists of many attributes such as branch of service, billet title, pay grade, clearance, attached command, etc. The following example illustrates two profiles:

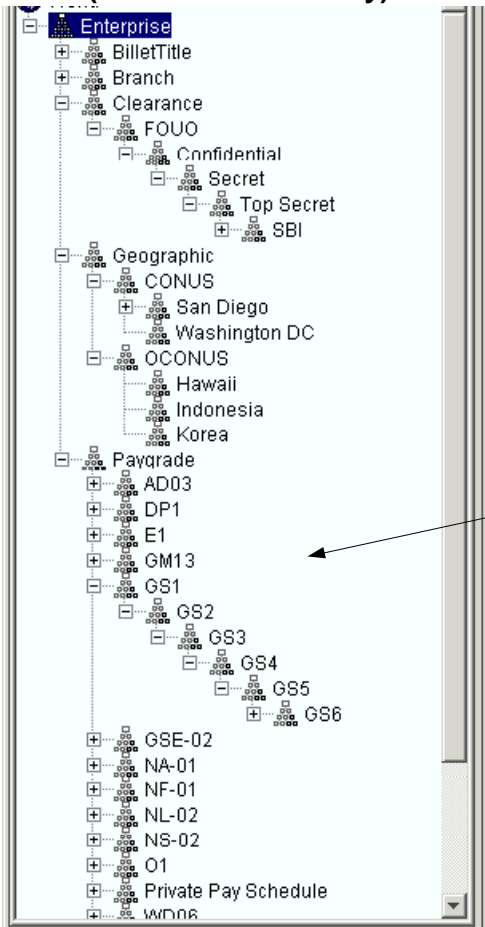
<u>Reference Categories</u>	<u>COMPACFLT Profile</u>	<u>SPAWAR Profile</u>
Assigned Command	N65	2424
Clearance	Secret	Top Secret
Paygrade	DP3	DP3
Service	DoD	DoD
Function	Developer	Network Engineer

A user could have one or more profiles. If a client had multiple user profiles, the client would have the option of selecting only one profile per session. The attributes on the session profile would determine the available resources. The creation and selection of these profiles must come from an authoritative entity.

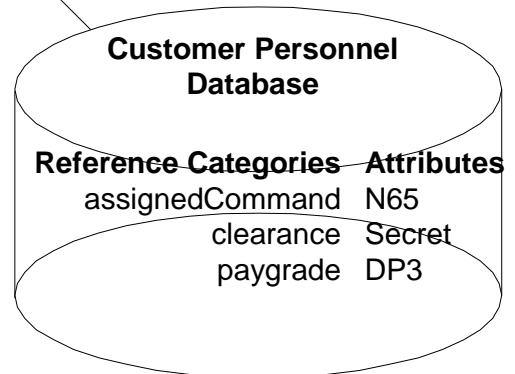
Conditioning User Profiles

A user profile has to be conditioned before it is passed to the RBAC for resource access evaluation. Conditioning involves converting user characteristics into distinguished name (DN) format. An RBAC Identity Manager queries customer personnel databases and obtains a series of categories (reference descriptor) with associated values. For example, AssignedCommand and N65; Clearance and Top Secret. These data pairs are then referenced with a customer meta-database (reference directory service) to produce a DN. The DNs are then appended to produce a user profile ready for RBAC evaluation. The diagram below illustrates the process.

Customer Meta-Database (Reference Directory)



Distinguished Name Generator



User Profile

ou=N65, ou=N6, ou=CPF, ou=assignedCommand, o=CPF
 ou=secret, ou=confidential, ou=fouo, ou=clearance, o=Enterprise
 ou=GS3, ou=GS2, ou=GS1, ou=Paygrade, o=Enterprise

Chapter 5

Chapter 5 Resource Roles

General

Resource roles are permissions within resources. In software applications or web services, resource roles represent accounts such as administrator, user, and guest privileges. The resource manager has the following three options when it comes to establishing resource role permissions:

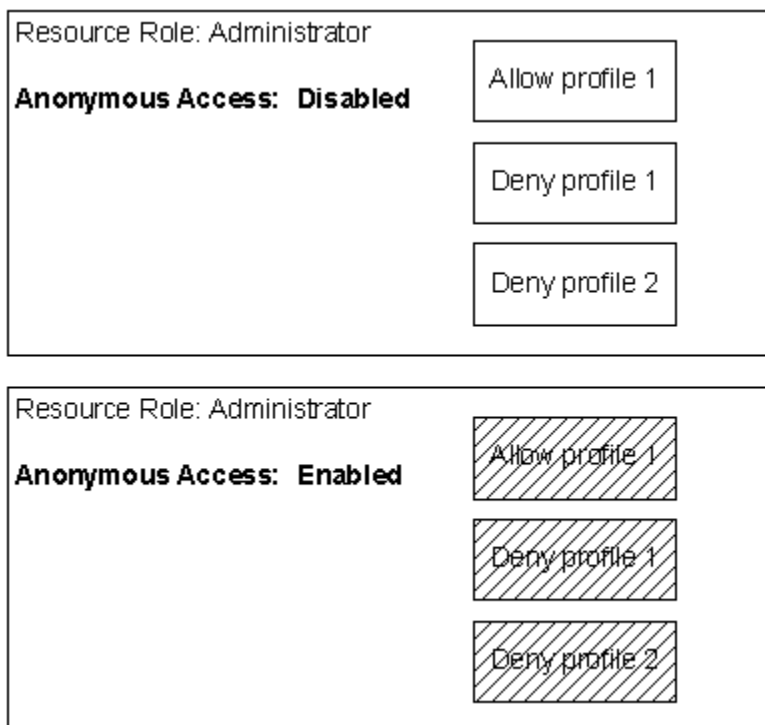
Disable – allows no one any access.

Conditional – allows certain personnel who satisfy a condition access.

Anonymous Access – allows unconditional access.

Anonymous Access

If a resource role is set to anonymous access, all assigned resource profiles are disabled and unconditional access is allowed into that resource role. See illustration below.



Role Levels

Role levels establish a hierarchy for resource roles. For example, a Resource with the following Resource Roles

<u>Resource Roles</u>	<u>Role Levels</u>
administrator	1
user	2
guest	3

would be assigned role levels 1, 2, and 3, respectively. A user with access rights to ALL resource roles can only select (via a client portal) the resource role with the lowest role level number, in this case **administrator**. Resource roles *user* and *guest* will not be available for selection because these roles are a higher number. Role levels have nothing to do with permissions; instead role levels dictate if a resource role will be visible for selection on a client portal.

If a client requires access to all resource roles then all resource roles should be assigned the same role level number.

<u>Resource Roles</u>	<u>Role Levels</u>
administrator	1
user	1
guest	1

In this example, resource roles **administrator**, **user**, and **guest** are assigned role level 1. It does not matter what role level is selected as long as all role levels have the same number. A user with access rights to ALL resource roles (**administrator**, **user**, and **guest**) will now be able to select all three resource roles from the portal.

By default, all resource roles are assigned the same role level 1 unless explicitly changed by a resource manager. Resource roles can be reassigned new role levels by selecting another integer from the combo box.

Chapter 6

Chapter 6 Resource Profiles

Resource Profile Overview

What are Resource Profiles?

A resource profile is a set of conditions that when compared to a user profile could allow or deny access to a resource role. Resource profiles are categorized as either Allow or Deny profiles. Resource profiles are established by a resource manager and are evaluated by the RBAC Rules Engine.

What is the Minimum Requirement to Gain Access?

Resource access is granted if:

- 1) all of the conditions in a Deny profiles do not match a user profile, and
- 2) all the conditions in an Allow profile matches a user profile

For example, a Project Tracker administrator account is assigned three Allow and two Deny profiles. If none of the Deny profiles produce a match and one out of the three Allow profiles produce a match with a user's profile, access is granted. However, if any Deny profile matches a user profile, access is denied and the evaluation process stops.

In What Order are Resource Profiles Evaluated?

The Rules Engine evaluates profiles in the following sequence:

- 1) Deny profile time constraint – if no time constraint is established or the time period has expired – proceed.
- 2) Deny profile – if no match is found – proceed.
- 3) Allow profile time constraint – if no time constraint is established or the time period has expired – proceed.
- 4) Allow profile – if match is found resource role is granted. If no match is found, no access is granted.

How Do Time Constraints Affect Resource Profiles?

A resource profile can be assigned time constraints. During a time constraint, the Rules Engine does not evaluate the respective resource profile. Essentially, a time constraint disables a resource profile during a certain period of time. For example, if a resource profile time constraint is set between 1700–1900 for every Monday and Tuesday, the resource profile will not be evaluated by the Rules Engine during those times.

Note: There are two types of time constraints (role and profile-based). A resource profile time constraint applies only to that profile. A resource role time constraint applies to ALL resource profiles assigned to it.

Do Conditions Have a Hierarchical Structure?

Yes. Conditions can be set on a specific (or exact) attribute such as GS12 pay grade or Secret clearance. Or a condition can include a group or subTree of attributes. For example, a subTree selection of GS12 encompasses pay grades GS12 - GS15. A subTree of Secret clearance encompasses clearances: Secret, Top Secret, and SBI.

Resource Profile Construct

A RM has the option to establish a set of conditions to grant or deny clients access to resource role (resource accounts). For example, a RM may establish a resource profile to access an "administrator" account for a Weapons Tracker application. The resource profile could contain the following set of conditions:

Resource Profile: NavMag Admin	
Reference Categories	Conditions
Paygrade	O1 and above
Clearance	Top Secret
AssignedCommand	NavMagHawaii

NavMag (Naval Magazine)

A descriptive name such as "NavMag Admin" would be appropriate to describe the resource profile. The RM could establish additional resource profiles to access the same resource role, administrator.

Each resource role will be assigned respective resource profiles. For example, the following two resource profiles could be established to access the "user" account for Weapons Tracker:

Resource Profile: CSP User	
Reference Categories	Conditions
Paygrade	E4 and above
Clearance	Secret
AssignedCommand	COMSUBPAC N2

COMSUBPAC/CSP (Commander, Submarine Force, U.S. Pacific Fleet)

Resource Profile: MIDPAC User	
Reference Categories	Conditions
Paygrade	GS11 & GS12
Clearance	SBI
AssignedCommand	MIDPAC N2

The more conditions a resource profile contains, the more restrictive the criteria to access. This is because at least one condition for each reference descriptor must match a user's profile. Ultimately security requirements will dictate the conditions to access a resource.

The figure below illustrates how:

One Allow and one Deny profile can grant or deny access to an **administrator** resource role.

One Allow and one Deny profile can grant access to a **user** resource role.

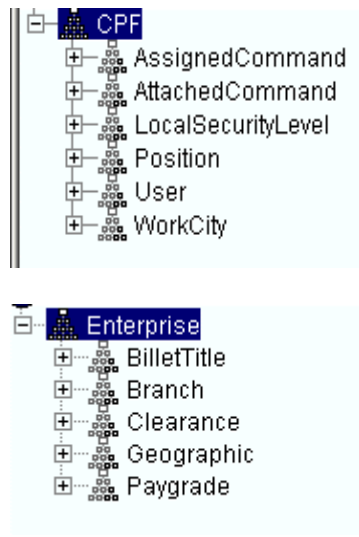
Three Allow profiles can grant access to a **guest** resource role.

Time constraints can also be attached to resource roles and resource profiles. Refer to chapter 7 for more details on time constraints

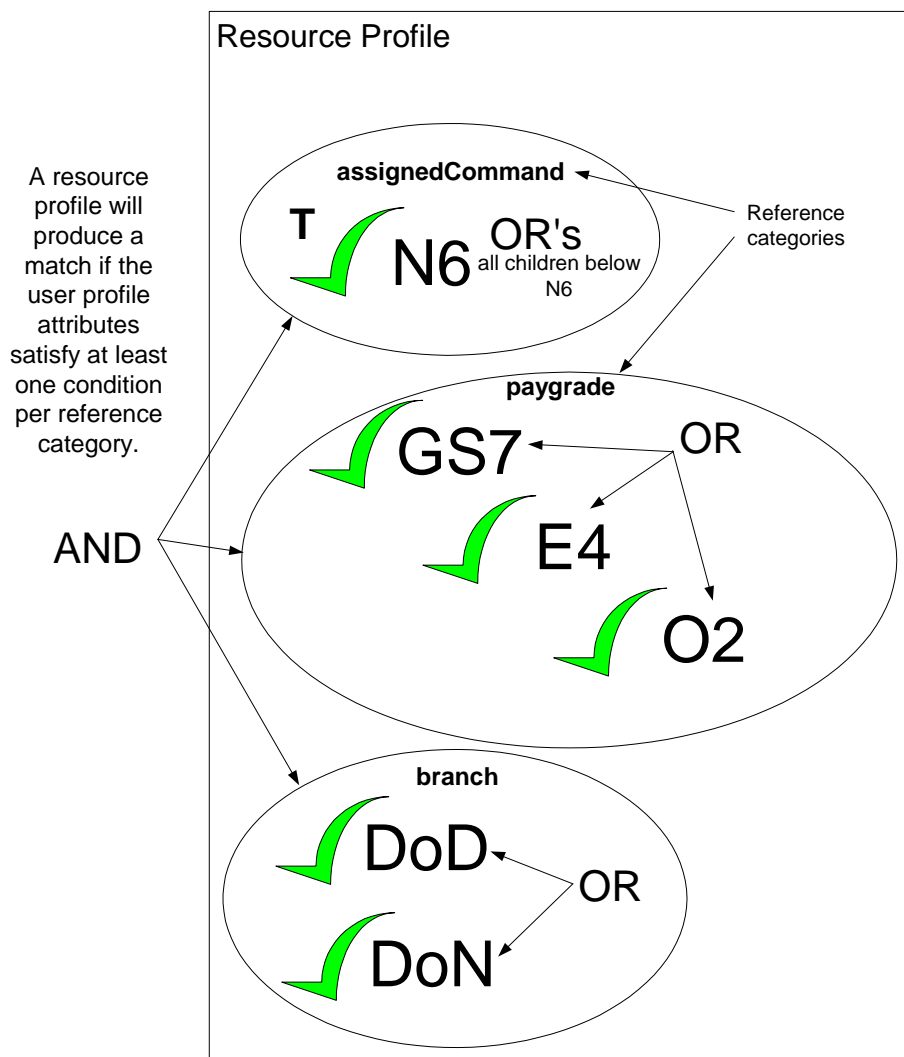
Resource Roles for Project Tracker	Resource Profiles		
Guest	CPF Guest T ✓ COMPACFLT	CSP Guest T ✓ COMSUBPAC	CNR Guests T ✓ COMNAVREG
			⊘ Tuesdays 1700 -2300
User	CPF N6 Users T ✓ CPF N6 T ✓ GS12	Deny Contr Users T ✓ CPF N6 Secret CONTR	
			⊘ Wednesday 1100 -1130
Administrator	CPF Admin ✓ CPF N65 T ✓ TS	Deny CPF N65 Admin T ✓ CPF N65 CONTR	
			⊘ Mon & Thurs 0800 -1300

Resource Profile Evaluation Logic

Resource managers select conditions (for resource access) from various reference directories. These reference directories can be local (i.e., CPF) or regional (i.e., Enterprise). Each reference directory contains a list of *reference categories* that categorize conditions. Refer to the CPF and Enterprise reference categories, shown below.



Multiple conditions belonging to a *reference descriptor* only have to match 1 user profile attribute to establish a match for that reference descriptor. The following diagram illustrates how conditions are evaluated within and among reference categories:



In another example, the following resource profile contains five conditions. Three of the five conditions belong to the Paygrade reference descriptor while the other two conditions, Secret and COMPACFLT N5, belong to the Clearance and AssignedCommand reference categories, respectively.

Resource Profile	
Reference Categories	Conditions
Paygrade	GS14, E1, O4
Clearance	Secret
AssignedCommand	COMPACFLT N5

A user with the following user profile

User Profile	
Reference Descriptor	Attribute
Paygrade	GS14
Clearance	Secret
AssignedCommand	COMPACFLT N5
BilletTitle	Developer
Branch	DoD

results in a match because all the resource profile conditions match the attributes contained in the user profile, including a single match of GS14 for the Paygrade reference descriptor.

However, conditions among ALL reference categories must match with a user profile in order to produce a resource profile match. For example, assume another user's profile consisted of the following:


User Profile	
Reference Categories	Attribute
Paygrade	E1
Clearance	Confidential
AssignedCommand	COMPACFLT N5
BilletTitle	Developer
Branch	DoD

In this example, a resource profile match will not result because not all conditions among ALL the reference categories matched.

Allow and Deny Resource Profiles

A [resource profile](#) is classified as an Allow or Deny profile. This section discusses the difference between the two.



Allow Resource Profiles

Allow profiles are associated with green checkmarks . Allow profiles store a list of condition(s) that are evaluated by the Rules Engine to grant access to a particular resource role (such as administrator, user). By default, if no Allow profile is established, no access is possible. A time constraint could be assigned to any resource profile. During a time constraint, the respective resource profile is not evaluated. Essentially, time constraints disable resource profiles during pre-configured times.

Since all conditions have to match a client's user profile attributes, access can become too restrictive if a resource profile contains too many conditions. Conditions are added to an Allow profile by:

- Selecting a resource profile from the Allow Profile window.
- Clicking on values from the reference directory information tree (DIT).

Deny Resource Profiles

Deny profiles are associated with red checkmarks   **Deny profiles are optional and complement Allow profiles.** For example, an Allow profile allows access to all CPF personnel. If you wish to restrict certain organizations within CPF, a Deny profile would be useful; for example, it would restrict all personnel in codes N2 and N7 within CPF. Establishing a Deny profile without an Allow profile accomplishes nothing. Deny profiles do exactly the opposite of Allow profiles. A Deny profile specifically denies access if a client's user profile attribute matches all conditions. The Rules Engine first evaluates all deny profiles before evaluating the Allow profiles. Just like Allow profiles, a Deny profile can also be assigned a time constraint.

Conditions are added to Deny profile by:

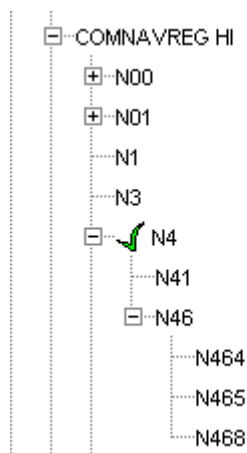
- Selecting a resource profile from the Deny profile window
- Clicking on values from the reference directory information tree (DIT).

Resource Profile Selection Types

Resource profile (Allow or Deny) conditions can be selected as follows:

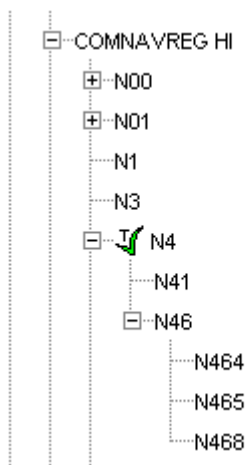
Exact Selections

Exact selections are represented by the green or red check marks. This type of selection is specific to a single condition. The illustration below indicates an exact selection of N4 only.



SubTree Selections

SubTree selections are represented by the green or red check marks and a letter "T". This type of selection selects the parent and all its children. The illustration below indicates a subTree selection for N4, which includes N41, N46, N464, N465, N468.




















Resource Profile Case Studies

The case studies below demonstrate the powerful RBAC condition setting capabilities for resource access.


Important rules of thumb when establishing resource profiles include the following:

- 1) A match occurs when ALL conditions in a resource profile (Allow or Deny profile) match a subset of the user profile.
- 2) Deny profiles are evaluated first. If a match occurs on a Deny profile, further profiles evaluated ceases and the user is denied access.
- 3) Time constraints essentially disable a resource profile from being evaluated during a certain period of time.

Resource Profiles			User Profiles	
Access	Reference Categories	Conditions	Reference Categories	Attributes
Deny Access Allows only personnel within N65 and not N651.	BilletTitle	 IT Program Manager	BilletTitle	IT Program Manager
	AssignedCommand	 CPF N65	AssignedCommand	CPF N651
	Clearance	 Secret	Clearance	Secret
			Paygrade	GS12
Deny Access Allows N651 personnel but must be Developers.	BilletTitle	 Developer	BilletTitle	IT Program Manager
	AssignedCommand	 CPF N65	AssignedCommand	CPF N651
	Clearance	 Secret	Clearance	Secret
			Paygrade	GS12
Allow Access ALL Allow profile conditions match user.	BilletTitle	 Developer,  Welder	BilletTitle	Developer
	AssignedCommand	 CPF N65,  CPF N2	AssignedCommand	CPF N651
	Clearance	 Secret	Clearance	Secret
			Paygrade	GS12
Deny Access (Tuesdays & Wednesdays 2200 -2300)	BilletTitle	 Developer,  Welder	BilletTitle	Developer
	AssignedCommand	 CPF N65,  CPF N2	AssignedCommand	CPF N651
	Clearance	 Secret	Clearance	Secret
Allow Access (all other times)	Time Constraint	 Tuesdays & Wednesday 2200-2300	Paygrade	GS12

Deny Access

All Deny profile conditions match user.

BilletTitle	 Developer,  Welder
AssignedCommand	 CPF N65,  CPF N2
Clearance	 Secret

BilletTitle	Developer
AssignedCommand	CPF N651
Clearance	Secret
Paygrade	GS12

AssignedCommand	 CPF N6,  CPF N2
Clearance	 Secret

Allow Access





(only on Mondays 1700 - 1800)

Deny Access

(all other times)









BilletTitle	 Developer,  Welder
AssignedCommand	 CPF N65,  CPF N2
Clearance	 Secret

BilletTitle	Developer
AssignedCommand	CPF N651
Clearance	Secret
Paygrade	GS12

AssignedCommand	 CPF N7,  CPF N2
Clearance	 Secret
Time Constraint	 Mondays 1700-1800

Allow Access









Since NOT all conditions of Deny profile match user. But ALL conditions of Allow profile do.

BilletTitle	 Developer,  Welder
AssignedCommand	 CPF N65,  CPF N2
Clearance	 Secret
AssignedCommand	 CPF N7
Clearance	 Secret
Paygrade	 GS12

BilletTitle	Developer
AssignedCommand	CPF N651
Clearance	Secret
Paygrade	GS12

Deny Access

Since a user profile does not match ANY Allow or Deny profile, access is denied.

BilletTitle	 Developer,  Welder
AssignedCommand	 CPF N65,  CPF N2
Clearance	 Secret
AssignedCommand	 CPF N7
Clearance	 Secret
Paygrade	 GS12

BilletTitle	Developer
AssignedCommand	CPF N3
Clearance	Secret
Paygrade	GS12

Deprecated Conditions

Conditions in resource profiles are selected from reference directories. User profiles are created from these same reference directories by use of the distinguished name (DN) Generator. The RBAC Rules Engine performs a comparison between these two profiles to determine resource access. Data changes to the reference directories due to a reorganization, salary structure, etc., will result in a mismatch and resource access will be denied.

For example, a resource manager establishes the following resource profile (consisting of three conditions) to access a resource called Project Tracker:

Resource Profile	
Reference Categories	Conditions
Paygrade	ou=GS2,ou=GS1,ou=Paygrade,o=Enterprise
Clearance	ou=secret,ou=confidential,ou=fouo,ou=Clearances,o=Enterprise
Command	ou=N651,ou=N65,ou=N6,ou=COMPACFLT,ou=Command,ou=CPF

After this resource profile is stored, an organization restructuring takes place, and the new distinguished name for N651 is changed to:

ou=N661, ou=N66, ou=N6, ou=COMPACFLT, ou=Command, ou=CPF

Clients will acquire a user profile based on the newly restructured organization as follows:

User Profile	
Reference Categories	Attribute
Paygrade	ou=GS2,ou=GS1,ou=Paygrade,o=Enterprise
Clearance	ou=secret,ou=confidential,ou=fouo,ou=Clearances,o=Enterprise
Command	ou=N661,ou=N66,ou=N6,ou=COMPACFLT,ou=Command, ou=CPF
BilletTitle	ou=Developer,ou=BilletTitle,ou=Enterprise
Branch	ou=DoD,ou=Branch,ou=Enterprise

The resource profile will not allow this user access because there is a mismatch with the command DN between user and resource profiles. The same result will occur if the user changes his command, but the reference directory data are unchanged. Such constraints furnish an automated safety feature to disallow access due to any changes. This capability epitomizes the important capabilities of a true RBAC system. These automated constraints now force resource managers to re-evaluate if resource access should be granted due to the latest changes in:

- a) A user whose characteristics (such as pay, organizations, etc.) have changed, or
- b) In an organization's restructuring.

In some cases, users will no longer be granted resource access because of the change.

If the reference directory data has changed, it will be difficult for the resource manager to pinpoint the obsolete conditions. The SEAC RBAC offers a capability that evaluates resource profile conditions with the current state of the reference directory. If the distinguished name of the condition cannot be found in the reference directory, this condition is classified deprecated, and it is highlighted in the RMC. The resource manager has to delete this deprecated condition or else the entire resource profile is rendered useless. After reconsidering new security issues, the resource manager may do one of two things:

- a) Replace the deprecated condition with another condition, or
- b) Not substitute the deprecated condition.

Global Conditions

The SEAC RBAC has the capability to globally define conditions. By default, selected conditions (within a resource profile) are in DN format. This means a user profile attribute (also in distinguished name format) has to equal the condition in order to produce a match. For example, the following represents a condition in the resource profile:

ou=N651,ou=N65,ou=N6,ou=COMPACFLT,ou=Command,ou=CPF

The following presents an attribute in a user profile:

ou=N651,ou=N65,ou=N6,ou=COMPACFLT,ou=Command,ou=CPF

The above scenario ONLY produces a match for N651 personnel within COMPACFLT. If a global condition were selected, it would only represent the relative distinguished name (RDN) of the condition, such as:

ou=N651

Under this scenario, a N651 user from ANY command would produce a match. Without this capability, resource managers would have to navigate under every command and select a consistent organization. Enterprise applications are usually tailored for a specific audience employed among many different commands or organizations. Using global conditions assists a resource manager in implementing enterprise access.

Chapter 7

Chapter 7 Time Constraints

Time Constraint Overview

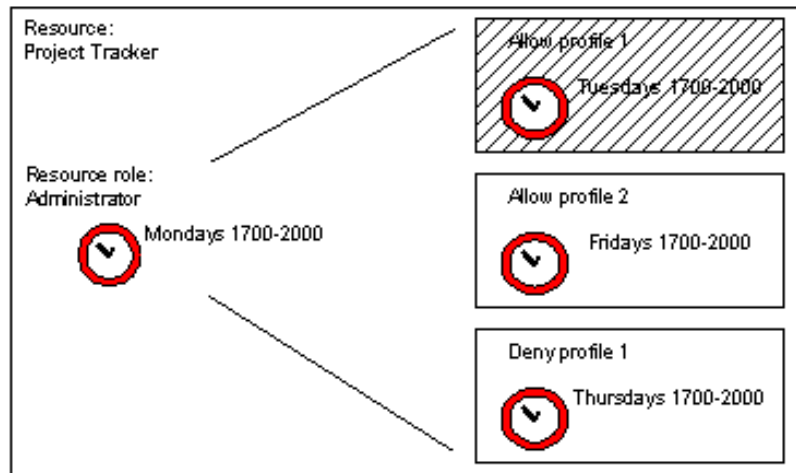
Time constraints essentially disable a resource role or resource profiles during designated times. Note: disabled resource roles and profiles are not evaluated by the Rules Engine. There are two types of time constraints:

- Resource Role Time Constraints
- Resource Profile Time Constraints

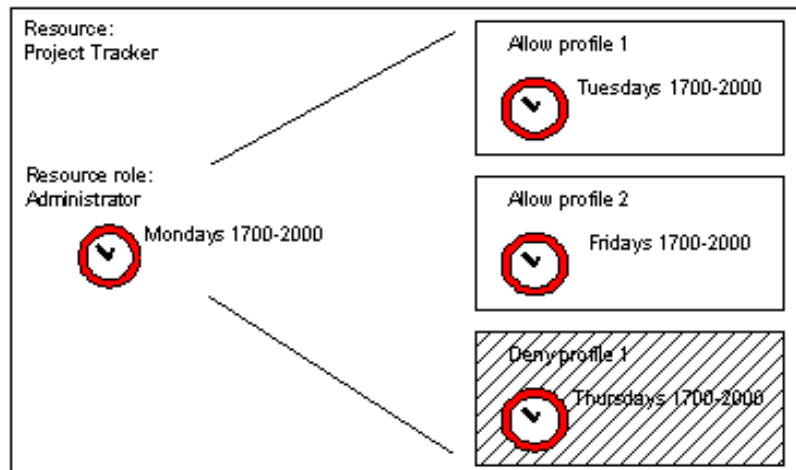
A resource profile time constraint applies only to the respective profile. A resource role time constraint applies to ALL resource profiles assigned to it. In the example below, the resource role administrator is assigned three resource profiles. Notice how time constraints disable the profiles.

In the example below, access to administrator would be denied to ALL users every Monday between 1700–2000. This is because no resource role is disabled during that time period. Resource profiles cannot be evaluated for a disabled resource role.

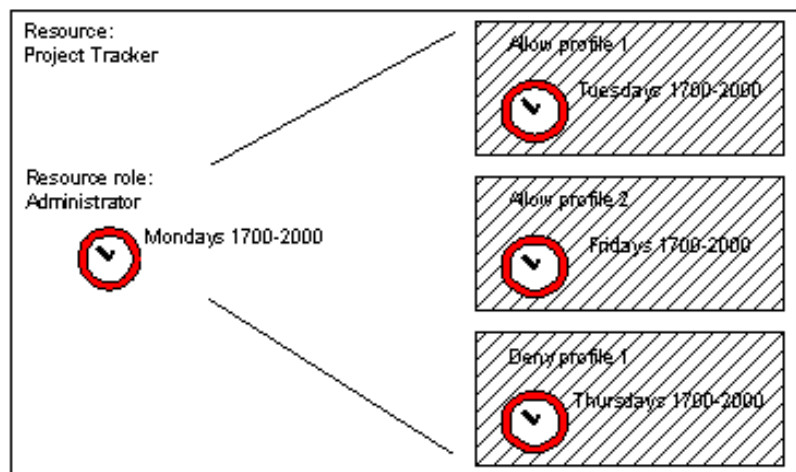
On Tuesday 1730
Allow profile 1 - disabled



On Thursday 1900
Deny profile 1 - disabled



On Monday 1830
All profiles - disabled



Chapter 8

Chapter 8 Security Levels

General

Security agencies such as Homeland Security and government and corporate Information Assurance (IA) agencies are authorized to impose security levels that may affect access to a wide range of resources by many personnel. Examples of security levels are:

- Homeland security advisory
- INFOCON (for U.S. military agencies)
- Corporate or private security advisories

Sudden changes in security levels may not allow sufficient time to modify ACLs. This could create possible security breaches by unauthorized personnel. Granularity of resource access may be required during certain security levels. For example, during INFOCONs C and D, only “administrator” and “superuser” account holders would be granted access, while all “guest” and “user” accounts would be denied access. An RBAC solution can accommodate these kinds of scenarios by pre-configuring resource access for all INFOCONs. Once an INFOCON state changes, the RBAC only evaluates the conditions pre-configured for the prevailing INFOCON. This chapter will focus on the INFOCON security levels, which consist of the following:

- INFOCON A
- INFOCON B
- INFOCON C
- INFOCON D

INFOCON A is the most relaxed security condition and INFOCON D the most stringent. INFOCONs are established by a cognizant IA agency. When IA imposes an INFOCON, the SEAC RBAC Rules Engine evaluates conditions only for that respective INFOCON state. The examples below illustrate this concept.

During INFOCON B

INFOCON A	Guest	CPF Guest	CSP Guest	CNR Guests
	User	CPF N6 Users	Deny Contr Users	
	Admin	CPF Admin	Deny CPF N65 Admin	
INFOCON B	Guest	CPF Guest	CSP Guest	CNR Guests
	User	CPF N6 Users	Deny Contr Users	
	Admin	CPF Admin	Deny CPF N65 Admin	
INFOCON C	Guest	CPF Guest	CSP Guest	CNR Guests
	User	CPF N6 Users	Deny Contr Users	
	Admin	CPF Admin	Deny CPF N65 Admin	
INFOCON D	Guest	CPF Guest	CSP Guest	CNR Guests
	User	CPF N6 Users	Deny Contr Users	
	Admin	CPF Admin	Deny CPF N65 Admin	

During INFOCON C

INFOCON A	Guest	CPF Guest	CSP Guest	CNR Guests
	User	CPF N6 Users	Deny Contr Users	
	Admin	CPF Admin	Deny CPF N65 Admin	
INFOCON B	Guest	CPF Guest	CSP Guest	CNR Guests
	User	CPF N6 Users	Deny Contr Users	
	Admin	CPF Admin	Deny CPF N65 Admin	
INFOCON C	Guest	CPF Guest	CSP Guest	CNR Guests
	User	CPF N6 Users	Deny Contr Users	
	Admin	CPF Admin	Deny CPF N65 Admin	
INFOCON D	Guest	CPF Guest	CSP Guest	CNR Guests
	User	CPF N6 Users	Deny Contr Users	
	Admin	CPF Admin	Deny CPF N65 Admin	

Notice how the resource profiles (assigned to resource roles) differ for each INFOCON. The RM pre-configures each resource role with various restrictions depending on various INFOCONs. The pre-configuration of resource access for each INFOCON establishes good security practices.

INFOCON Aware Selection

In the Resource Management Console (RMC), INFOCON Aware is unselected by default. If the RM wishes to establish various INFOCON states, INFOCON Aware is checked and conditions established for each respective INFOCON (A, B, C and D). If no condition(s) are established for a particular INFOCON, then resource access will not be allowed. For example, say INFOCON Aware is selected and under INFOCON A anonymous access is enabled and under INFOCON B a resource profile allows CPF personnel access. The following consequences will occur under the various INFOCONs:

INFOCON A – any user can access this resource since anonymous access is enabled.

INFOCON B – only CPF personnel can access this resource.

INFOCON C – no one can access resource.

INFOCON D – no one can access resource.

INFOCON Aware Unselection

If the RM does not have a requirement to establish various conditions for different INFOCONs, then INFOCON Aware should remain unchecked. **An unchecked INFOCON Aware equals INFOCON A.** This way, if the RM later decides to implement various INFOCON restrictions, the conditions already established will apply to INFOCON A. If INFOCON Aware remains unchecked, the established conditions are always evaluated by the Rules Engine regardless of the prevailing INFOCON state.

Case Studies

Case Study:

Resource: Time Tracker

Role: Guest (Access: INFOCON A)
(Deny: INFOCON B, C, D)

Role: User

Resource Profile: CPF Personnel (Applicable for INFOCON A, B)

Resource Profile: Commander, Naval Region (COMNAVREG) Personnel (Applicable for INFOCON A, B)

Role: Administrator

Resource Profile: CPF Mgmt (Applicable for INFOCON A, B, C, D)

Resource Profile: COMNAVREG Mgmt (Applicable for INFOCON A, B, C)

During INFOCON A:

All enterprise personnel will have access to role: Guest access on resource: Time Tracker.

CPF and COMNAVREG personnel will have access to role: User on resource: Time Tracker.

CPF and COMNAVREG management will have access to role: Administrator on resource: Time Tracker.

During INFOCON B:

All enterprise personnel will be denied total access on resource: Time Tracker.

CPF and COMNAVREG personnel will be denied access to role: User on resource: Time Tracker.

CPF and COMNAVREG management will have access to role: Administrator on resource: Time Tracker.

During INFOCON C:

All enterprise personnel will be denied total access on resource: Time Tracker.

CPF and COMNAVREG personnel will be denied total access on resource: Time Tracker.

CPF and COMNAVREG management will have access to role: Administrator on resource: Time Tracker.

During INFOCON D:

All enterprise personnel will be denied total access on resource: Time Tracker.

CPF and COMNAVREG personnel will be denied access to role: User on resource: Time Tracker.

COMNAVREG management will be denied total access on resource: Time Tracker.

CPF management will have access to role: Administrator on resource: Time Tracker.



SPAWAR
Systems Center
San Diego

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

Approved for public release:
distribution is unlimited.



COMPACFLT SEAC RBAC

Commander, Pacific Fleet (COMPACFLT) Secure Enterprise Access Control (SEAC) Role Based Access Control (RBAC)

Point of Contact:
Richard Fernandez
(808) 474-9270



The information contained herein is considered U.S. Government Proprietary and may be related to one or more U.S. Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

SD 541, June 2004

SSC San Diego

San Diego, CA 92152-5001

Approved for public release; distribution is unlimited.



COMPACFLT SEAC RBAC

The SEAC RBAC is available at:

<http://www.spawar.navy.mil/sti/publications/pubs/td/3182/td3182con.pdf>

References:

<http://csrc.nist.gov/rbac/>

For comments contact:

Richard Fernandez

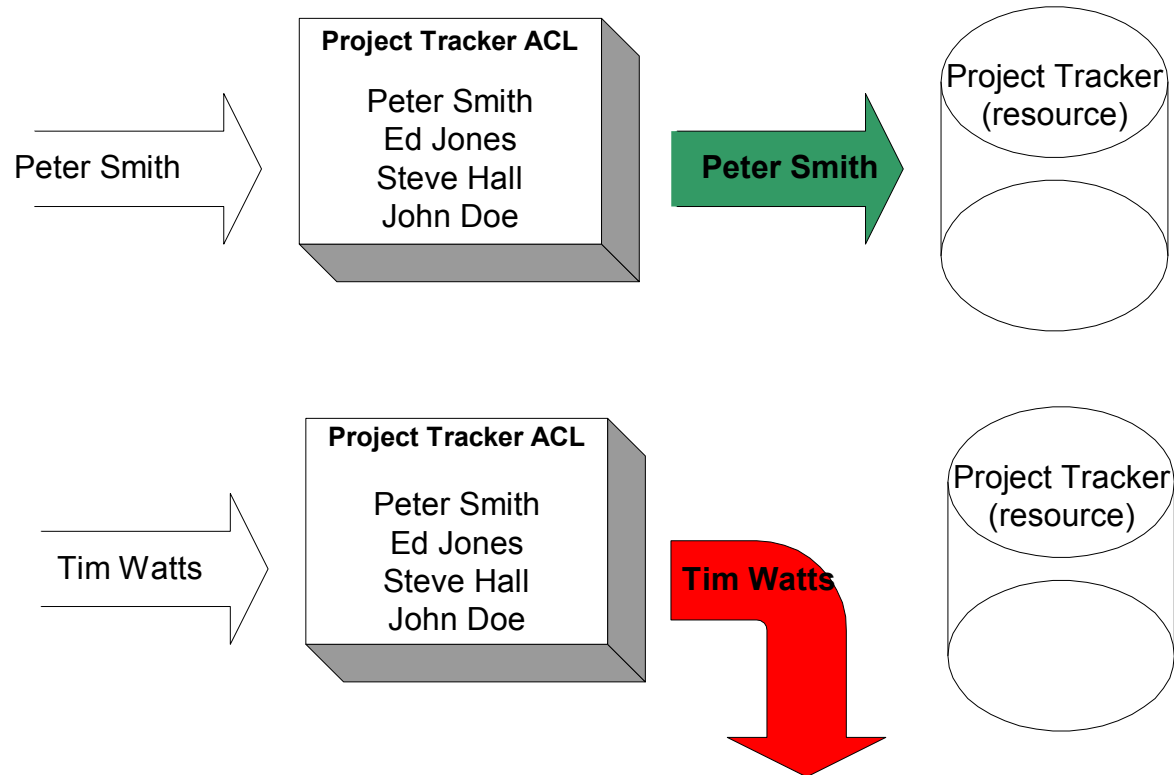
(808) 474-9270

Richard.R.Fernandez@navy.mil



Access Control Lists (ACL)

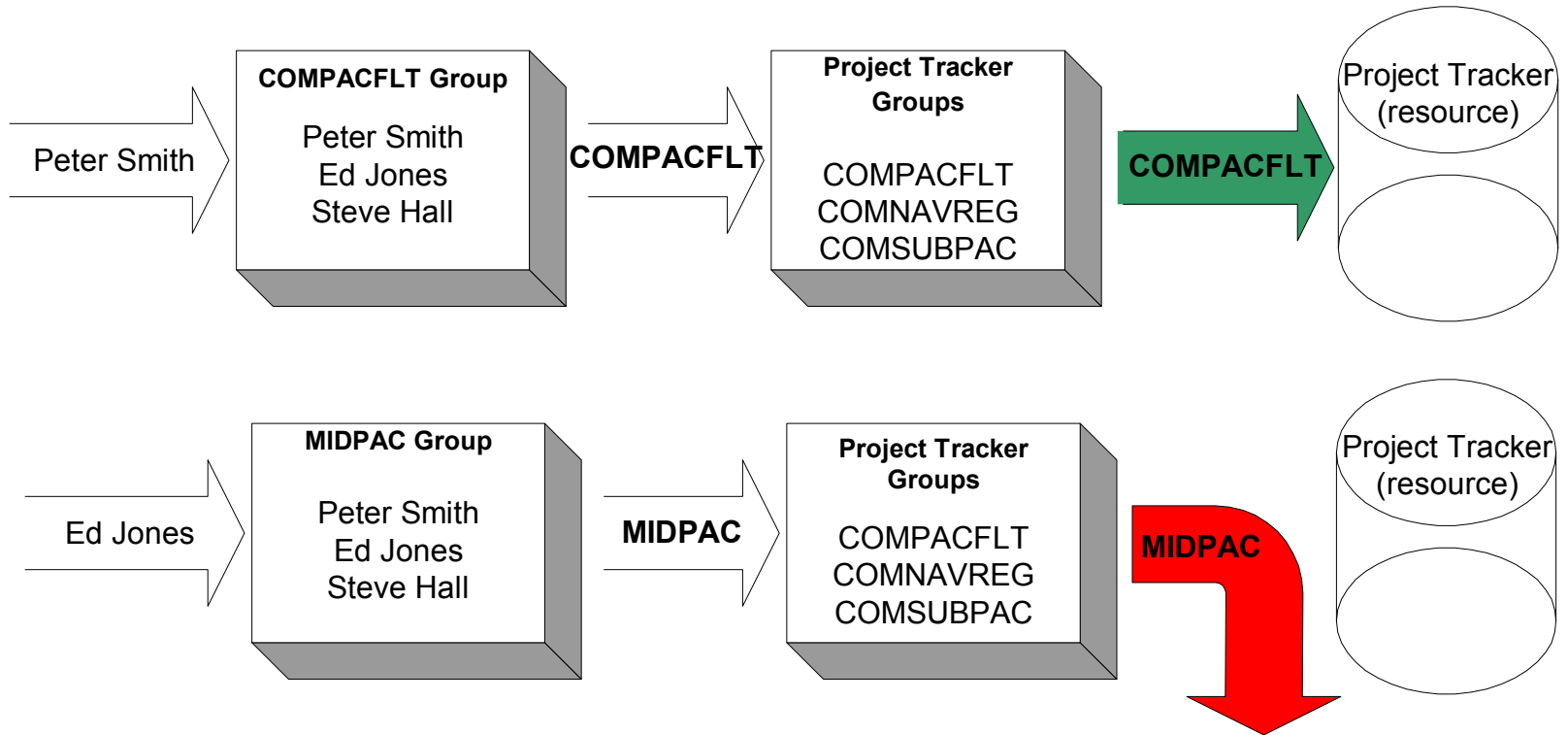
User name or unique identifier associates access to resources





Groups

User associated to a group and group associated to resources





Essentials for resource access

Necessary requirement to access resources:

- Not a user name
- Not a unique identifier
- Not a group association

- List of user characteristics



What are user characteristics

User characteristics (user profile)

- Where client works: **organization**
- What security credentials: **clearance**
- What pay category: **pay grade**
- What branch : **service**
- What vocation: **job function**
- etc



Examples of User Profiles

- User profile is a unique list of user characteristics.
- A client may have more than one user profile.
- User attributes should be compiled from an authoritative data source(s) on a real-time basis.

<u>Categories</u>	<u>COMPACFLT</u>	<u>USNR</u>
Organization:	CPF N65	Naval Intel
Clearance:	Secret	Top Secret
Paygrade:	DP3	02
Service:	DoD	DoNR
Function:	Program Manager	Intelligence



Impact on resource access

The following can affect resource access:

- Transfer to another organization
- Loss of security clearance
- Change in job title
- Job promotion

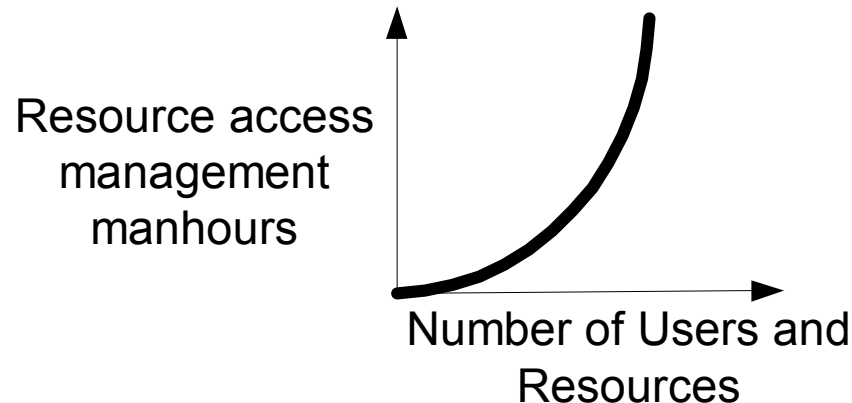


Problems with ACLs and Groups

Maintaining an updated ACL or group is time consuming.

Situation worsens when:

- Number of users increase
- Number of resources increase





NIST RBAC compliance

Because of ACL and group limitations:

The National Institute of Standards and Technology (NIST) has declared RBAC an American National Standard - ANSI INCITS 359-2004 (approved 19 Feb 04)



NIST RBAC standard

Definitions:

Users and Roles: *"...access decisions are based on the roles that individual users have as part of an organization.*

"Access rights are grouped by role name..."

Role hierarchies: *"Under RBAC, roles can have overlapping responsibilities and privileges;*

Roles and Operations: *"Organizations can establish the rules for the association of operations with roles.*



Access control comparison

How access control solutions can simultaneously evaluate user characteristics.

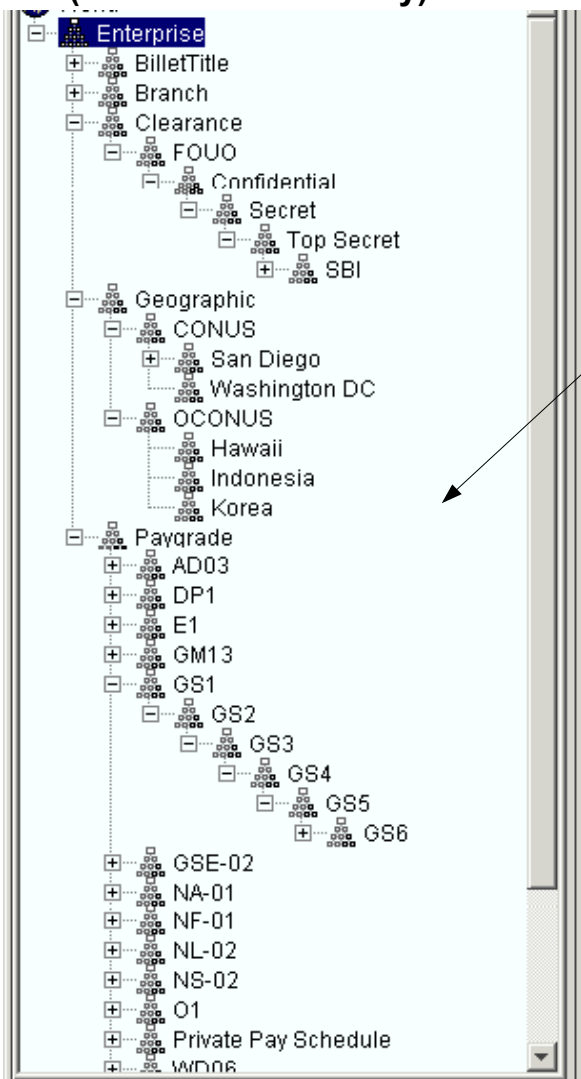
	User Characteristics	
	Number of user characteristics evaluated	Hierarchal evaluation of user characteristics
ACLs	0	No
Groups	1	Yes/No
NIST RBAC	1	Yes
SEAC RBAC	Unlimited	Yes

Note: A hierarchal structure offers inheritance capabilities.

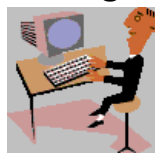


How the SEAC RBAC works

Customer Meta-Database (Reference Directory)



RBAC Condition Manager



Step 1:

Resource manager establishes
a set of conditions to access a
resource.

These set of conditions
represent a **resource profile**.

Resource Profile

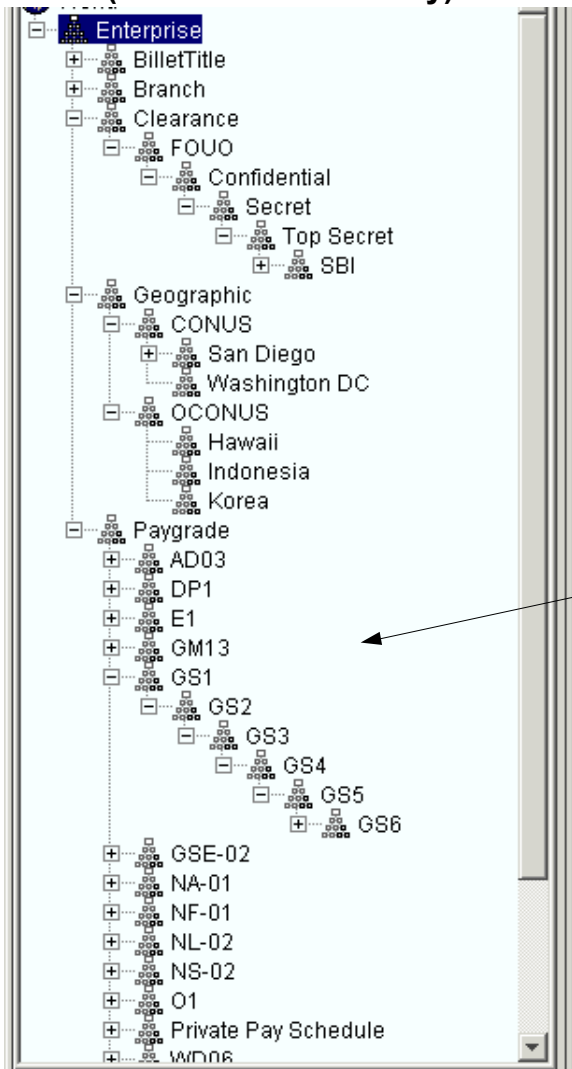
✔ ou=N65, ou=N6, ou=CPF, ou=assignedCommand, o=CPF
✔ ou=secret, ou=confidential, ou=fouo, ou=clearance, o=Enterprise

RBAC Resource Directory



How the SEAC RBAC works

Customer Meta-Database (Reference Directory)



Customer User Profile Manager Interface



Distinguished Name Generator

Step 2:

An effective RBAC requires real-time creation of user profile(s) from authoritative data source(s).

Customer Personnel Database

Reference Categories	Attributes
assignedCommand	N65
clearance	Secret
paygrade	GS3

User Profile

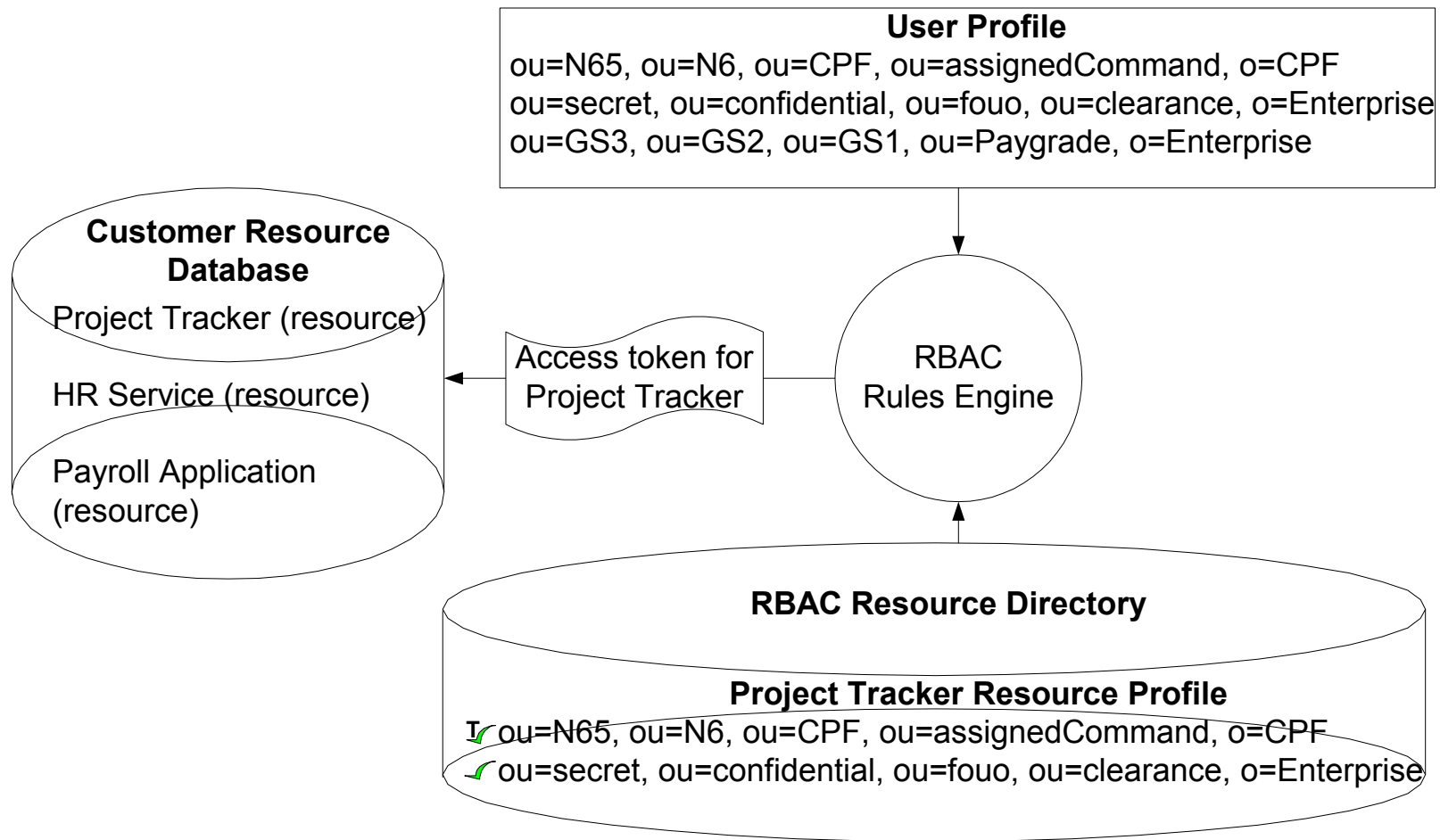
ou=N65, ou=N6, ou=CPF, ou=assignedCommand, o=CPF
ou=secret, ou=confidential, ou=fouo, ou=clearance, o=Enterprise
ou=GS3, ou=GS2, ou=GS1, ou=Paygrade, o=Enterprise



How the SEAC RBAC works

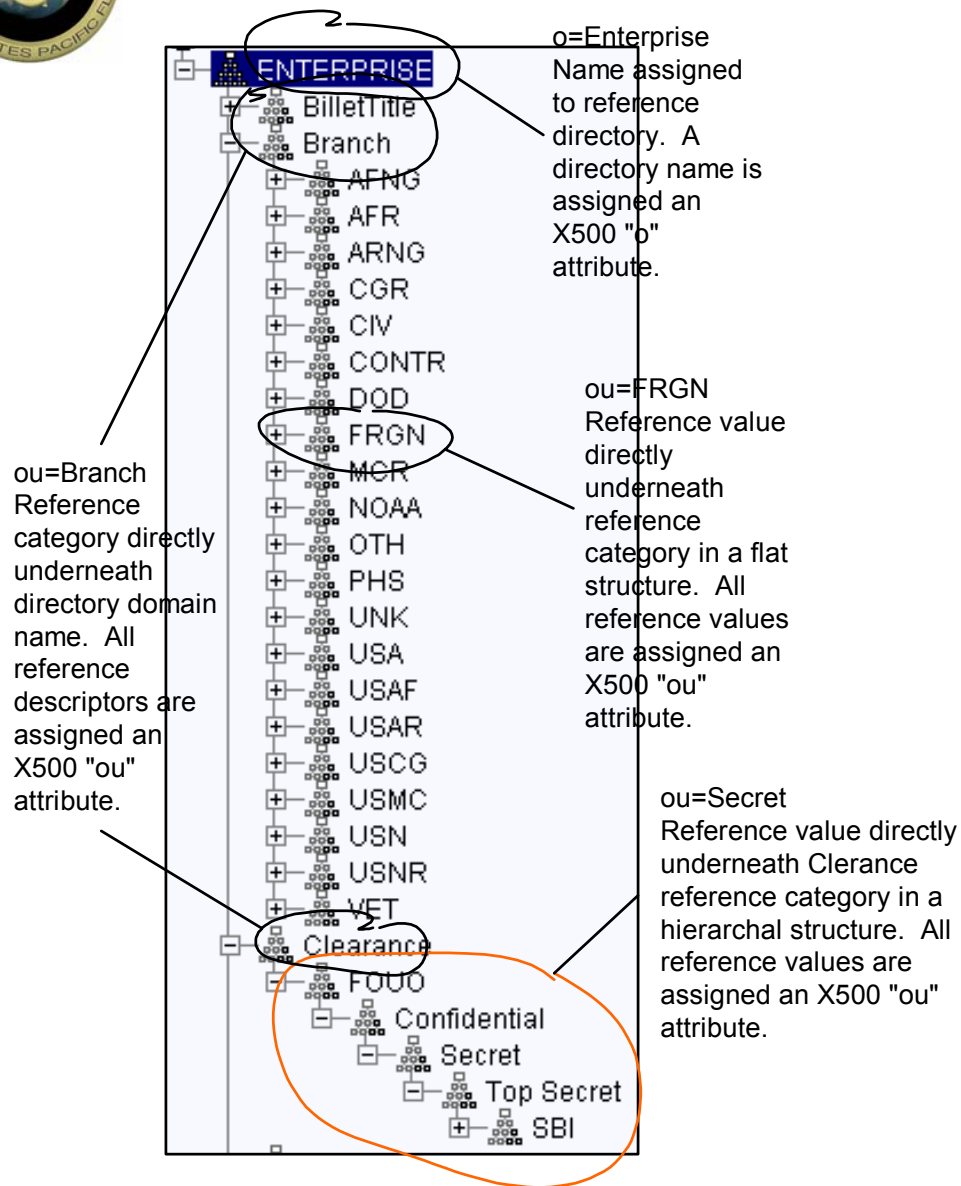
Step 3:

The RBAC Rules Engine compares User and Resource Profiles to determine resource access.








Reference directory standard specifications



- Customer meta-database
- LDAP v 3/DSML directory
- X500 class objects
 - organization
 - organizationalUnit
- Scalable
 - unlimited entries
 - modifications allowed
- Structure designation
 - domain
 - reference category
 - values
- Structure
 - flat
 - hierarchal
- Maintained
 - local commands
 - regional commands



SEAC RBAC – Resource profiles

Resource Roles for Project Tracker	Resource Profiles		
Guest	CPF Guest T ✓ COMPACFLT	CSP Guest T ✓ COMSUBPAC ✓ DoD	CNR Guests T ✓ COMNAVREG  Tuesdays 1700 -2300
User	CPF N6 Users T ✓ CPF N6 T ✓ GS12  Mon & Thurs 0800 -1300	Deny Contr Users T ✗ CPF N6 ✗ Secret ✗ CONTR	
Administrator	CPF Admin ✓ CPF N65 T ✓ TS	Deny CPF N65 Admin T ✗ CPF N65 ✗ CONTR  Mon & Thurs 0800 -1300	

- Resource roles
- Allow & Deny profiles
- Exact and subtree conditions
- Time constraints



SEAC RBAC – Security levels

During INFOCON B

INFOCON A	Guest	CPF Guest ✓	CSP Guest ✓	CNR Guests ✓
	User	CPF NB Users ✓	Deny CNR Users ✓	
	Admin	CPF Admin ✓	Deny CPF NIS Admin ✓	
INFOCON B	Guest	✓	✓	✓
	User	✓	✓	
	Admin	✓	✓	
INFOCON C	Guest	✓	✓	✓
	User	✓	✓	
	Admin	✓	✓	
INFOCON D	Guest	✓	✓	✓
	User	✓	✓	
	Admin	✓	✓	

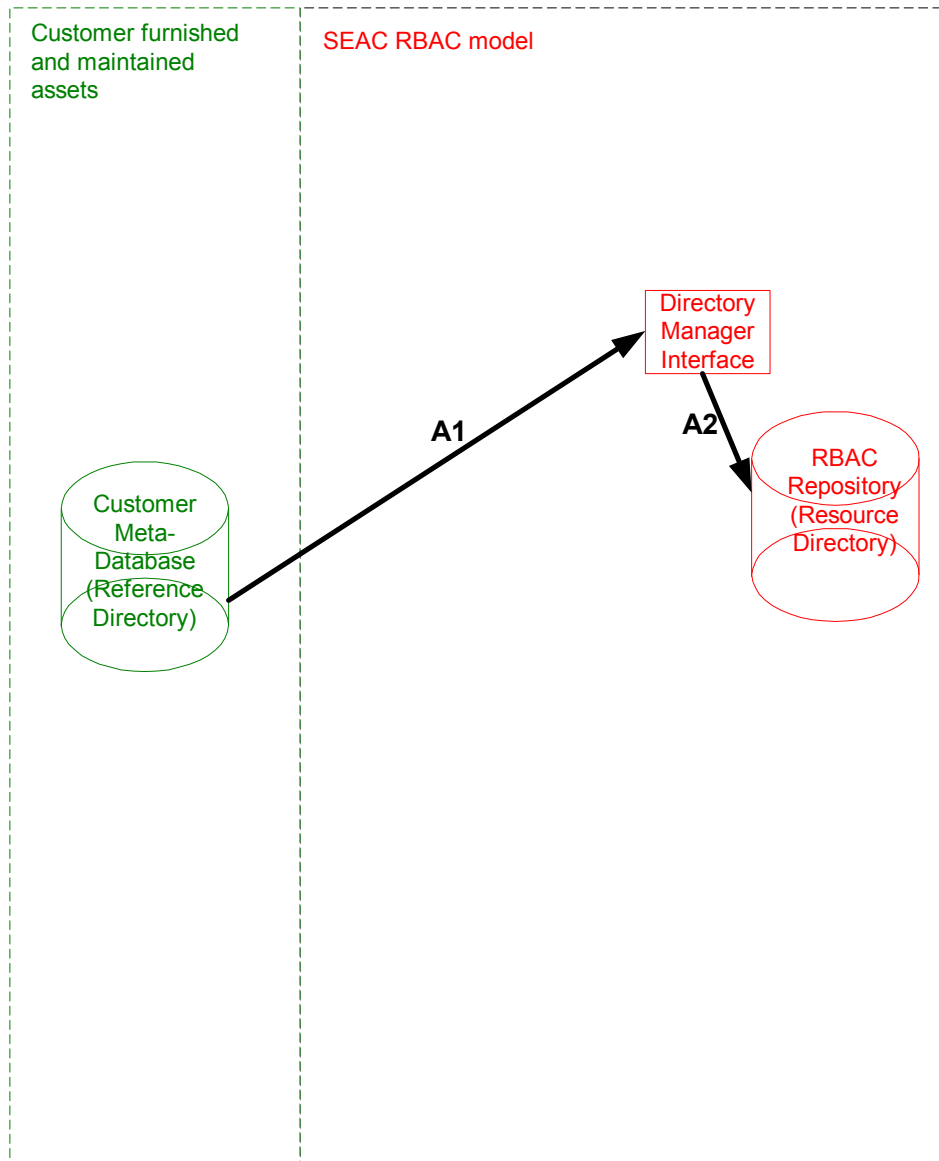
During INFOCON C

INFOCON A	Guest	✓	✓	✓
	User	✓	✓	
	Admin	✓	✓	
INFOCON B	Guest	✓	✓	✓
	User	✓	✓	
	Admin	✓	✓	
INFOCON C	Guest	✓	✓	✓
	User	✓	✓	
	Admin	✓	✓	
INFOCON D	Guest	✓	✓	✓
	User	✓	✓	
	Admin	✓	✓	

- Pre-configure conditions under each security level.
- RBAC Rules Engine evaluates only conditions for prevailing security level.



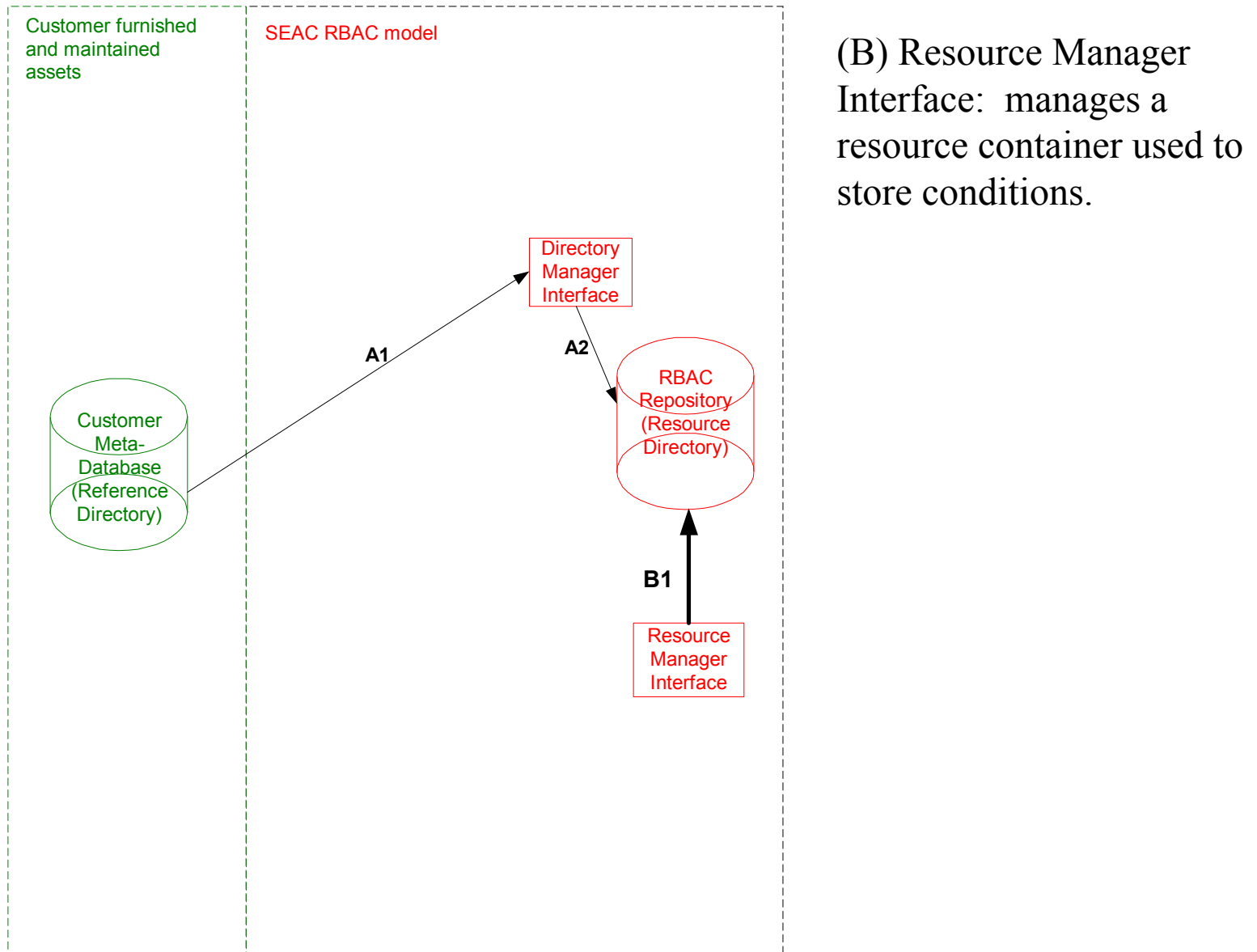
SEAC RBAC - Model



(A) Directory Manager Interface: manages reference directory referrals.

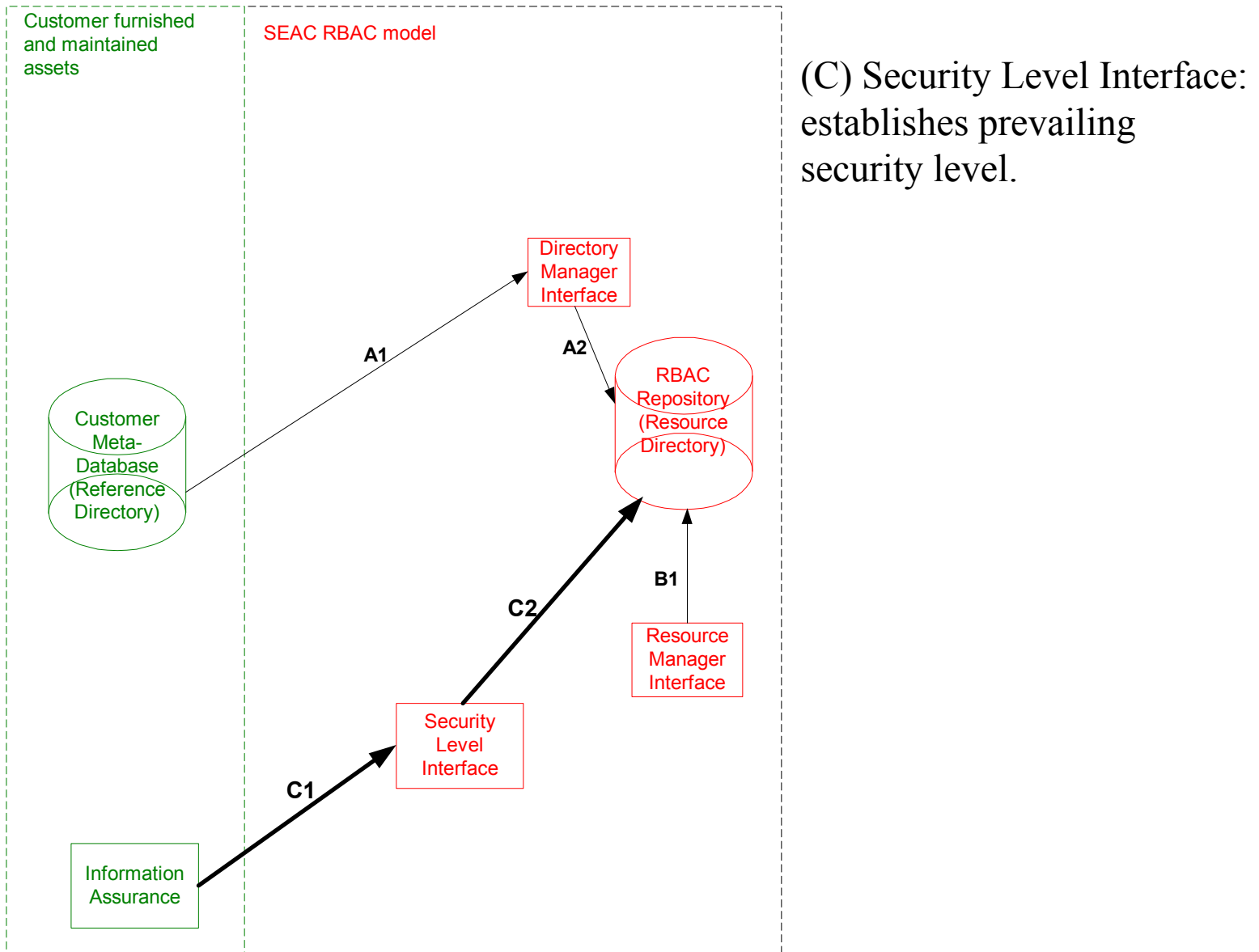


SEAC RBAC - Model



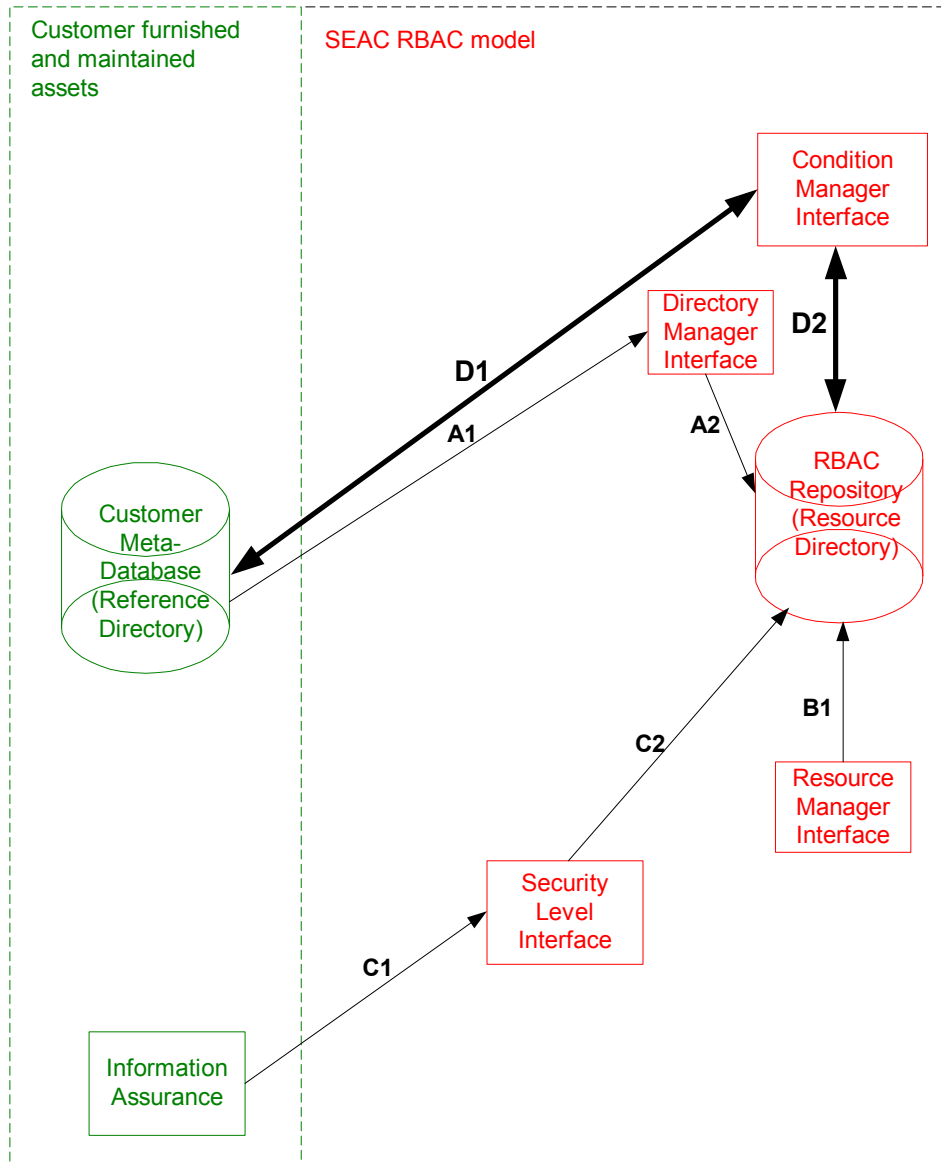


SEAC RBAC - Model





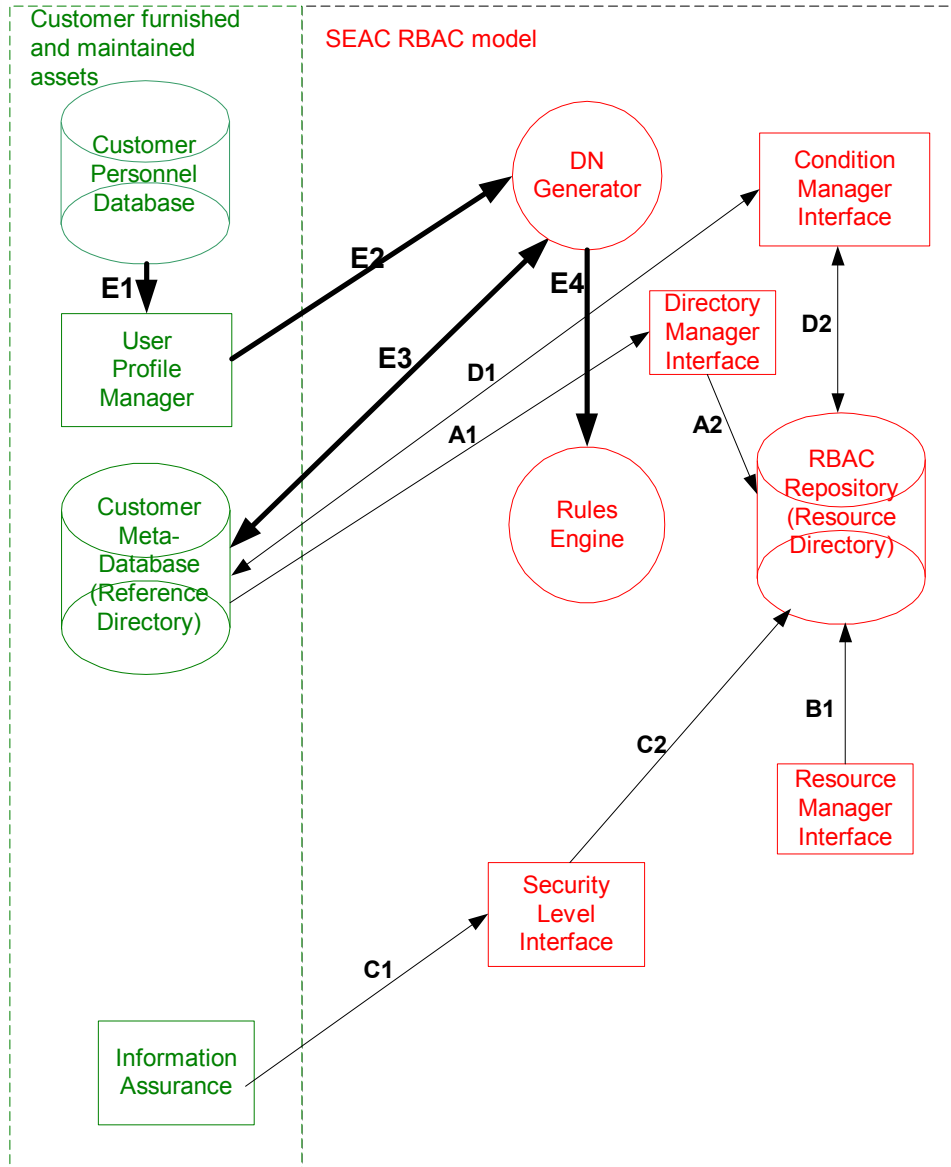
SEAC RBAC - Model



(D) Condition Manager Interface: establishes conditions to access resources.



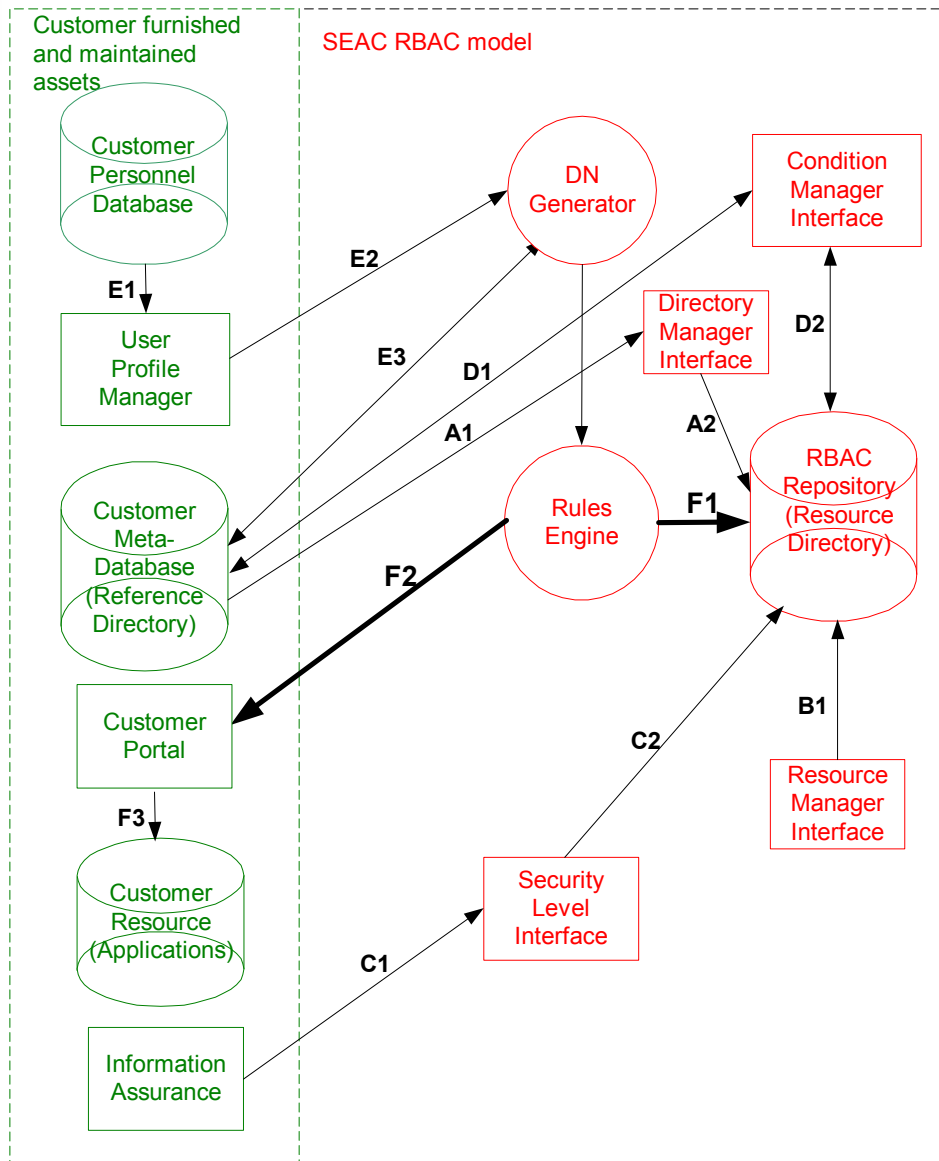
SEAC RBAC - Model



(E) User profile manager:
user profile selection and DN
formatting.



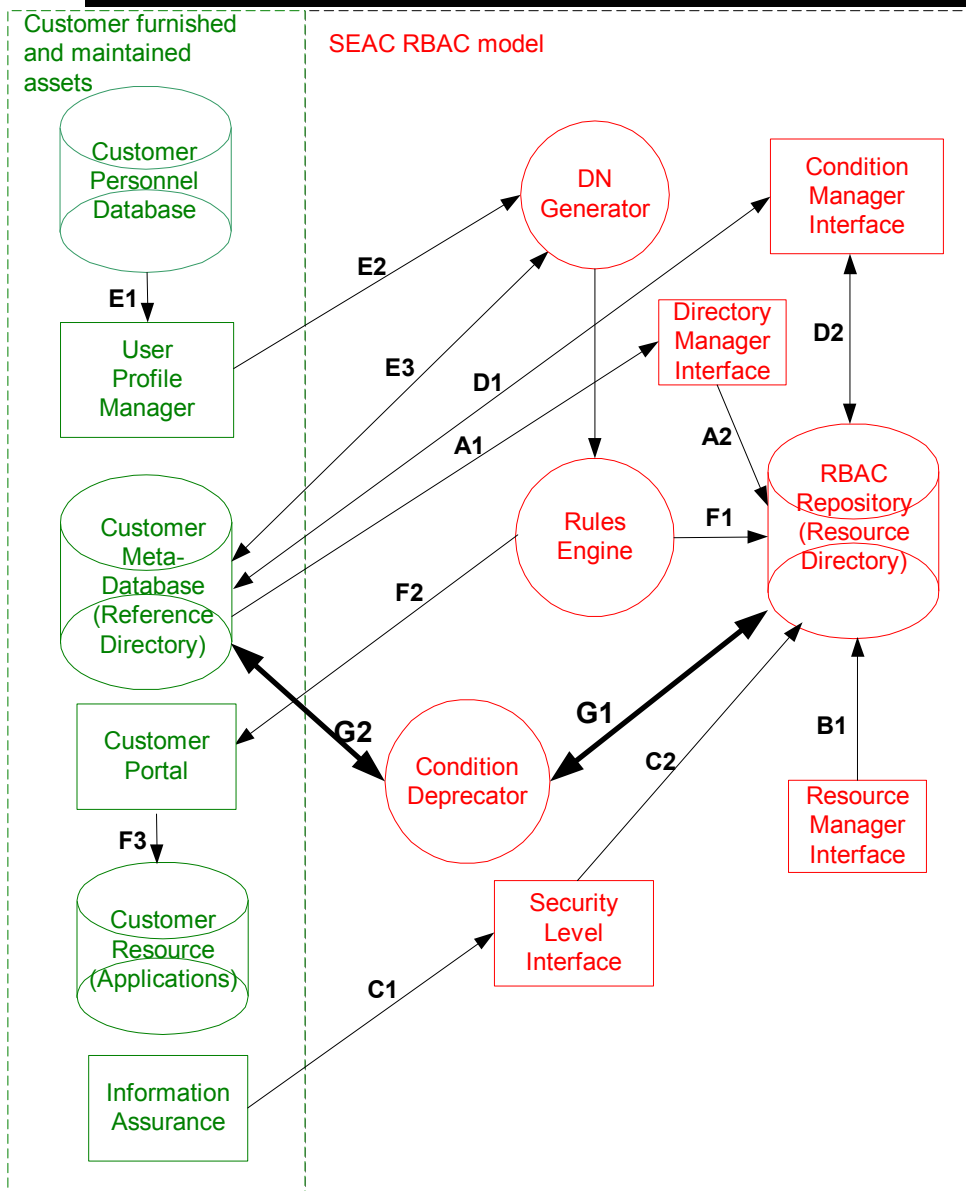
SEAC RBAC - Model



(F) Rules Engines: evaluates user and resource profiles to determine resource access.



SEAC RBAC - Model

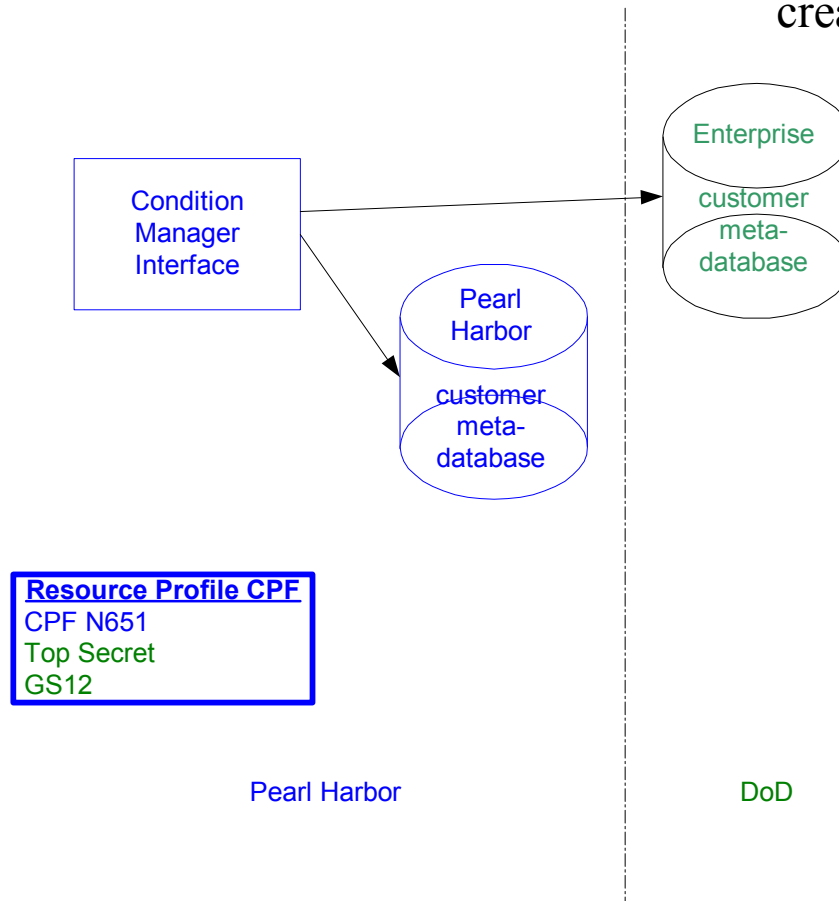


(G) Condition deprecation: scans reference directories and compares resource profiles for any changes.



SEAC RBAC - Interoperability

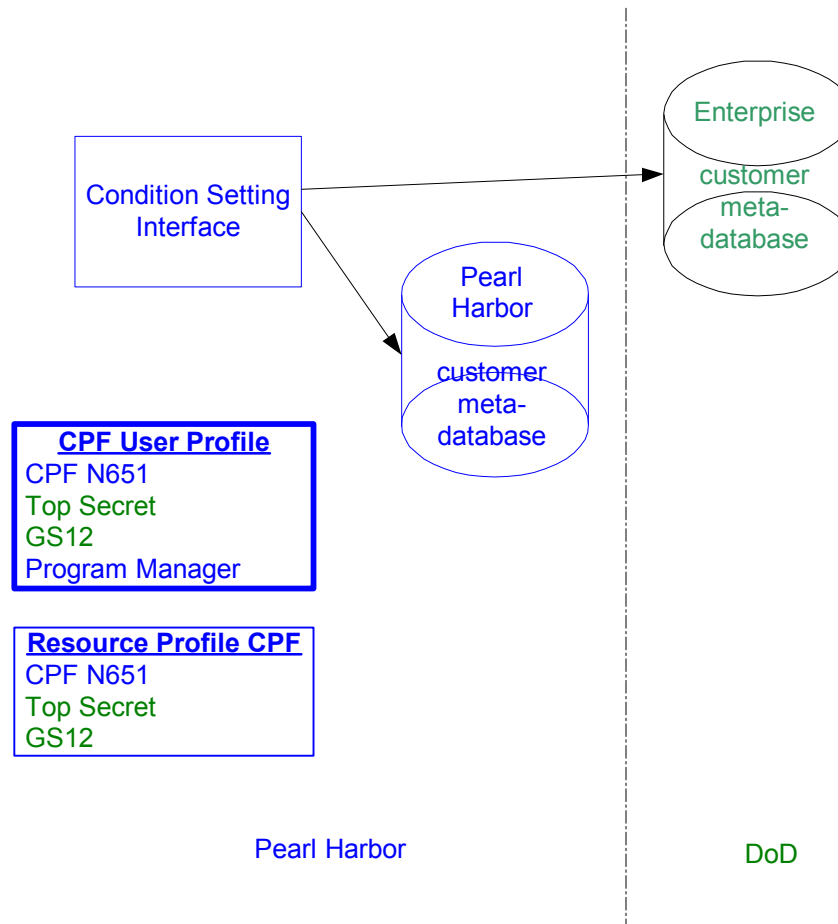
Pearl Harbor: resource profile created for local resource access.





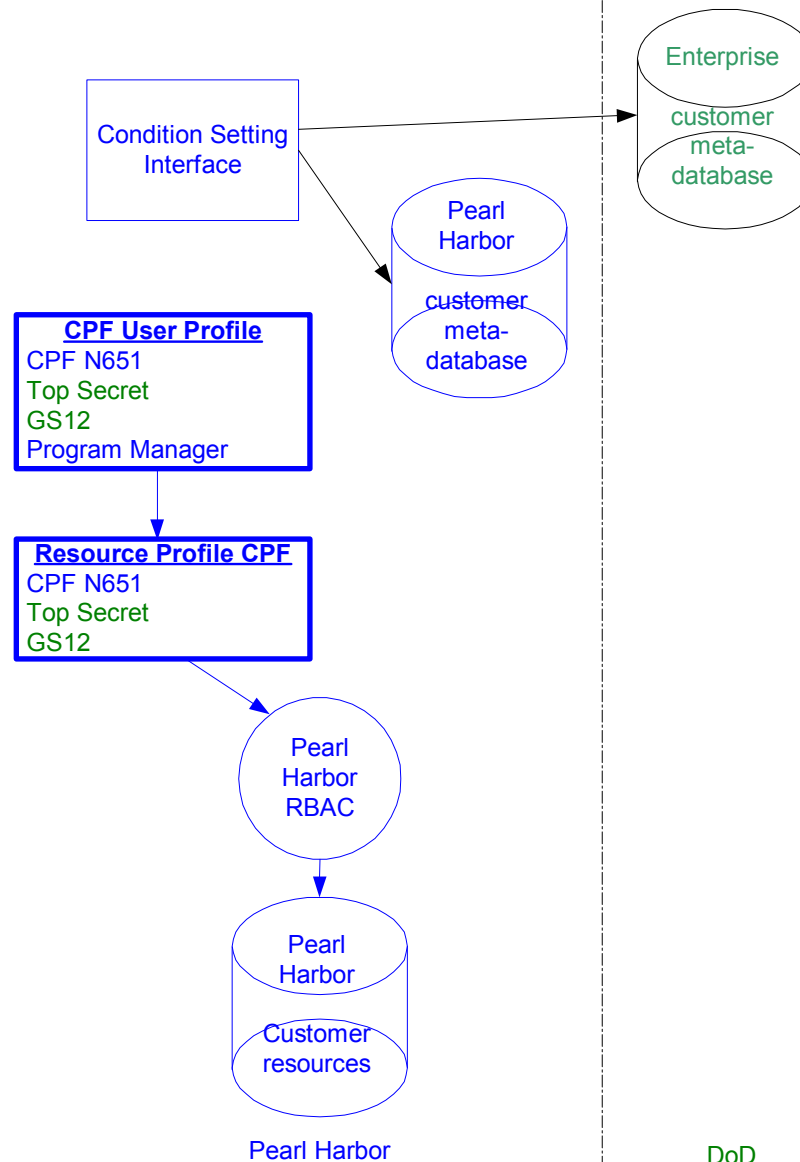
SEAC RBAC - Interoperability

Pearl Harbor: local user profile is generated to access a local resource.





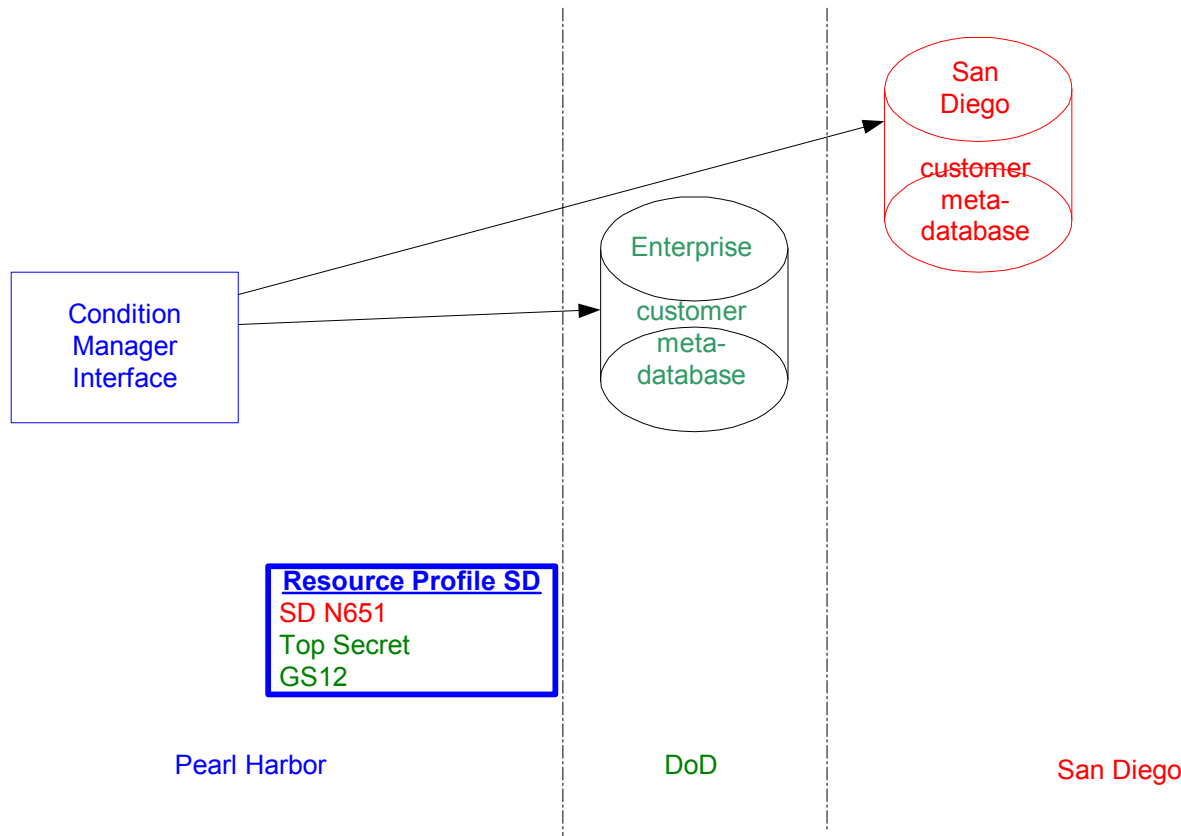
SEAC RBAC - Interoperability



Pearl Harbor: user and resource profiles are evaluated by rules engine to determine local resource access.



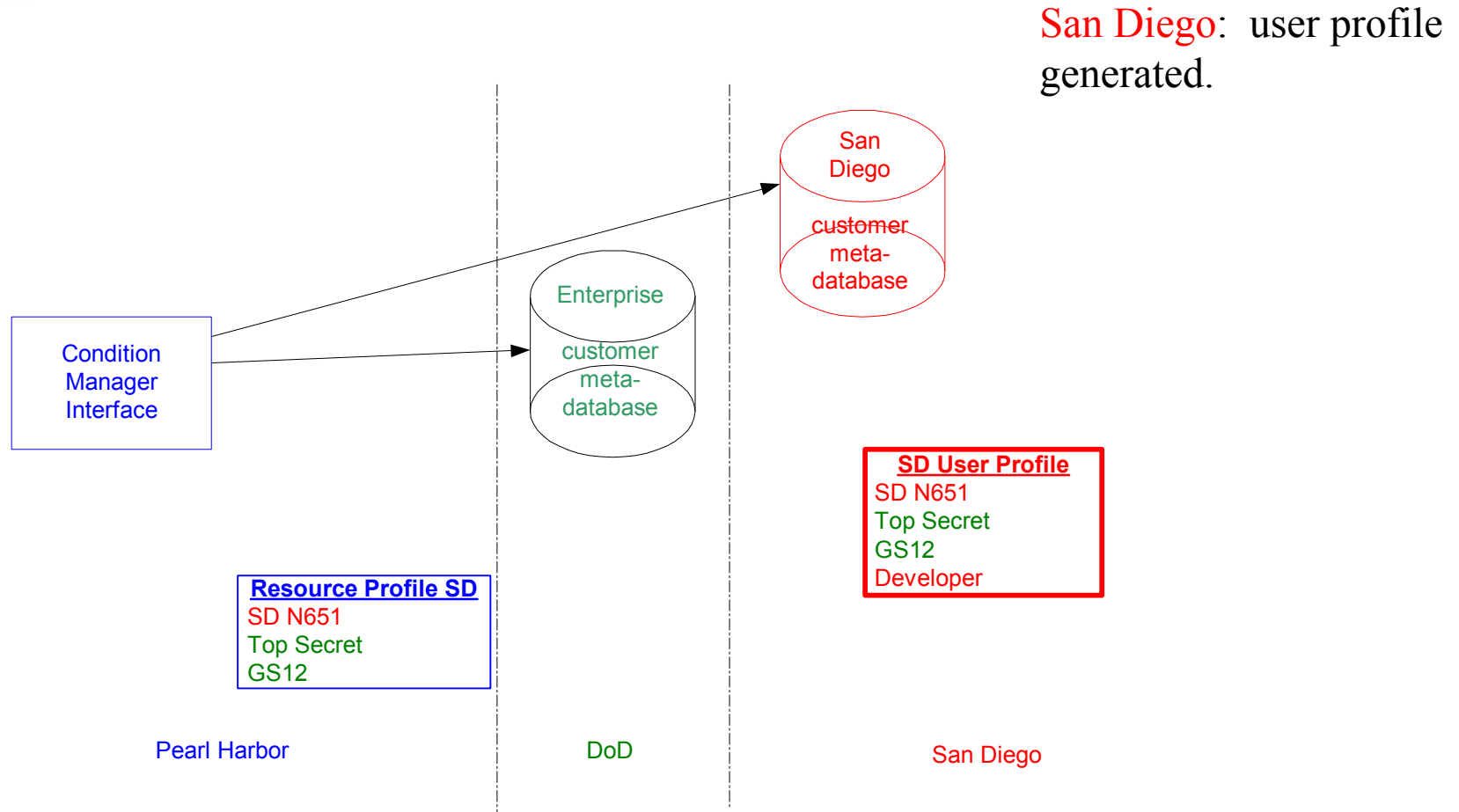
SEAC RBAC - Interoperability



Pearl Harbor: A resource profile to allow remote users access to local resources.

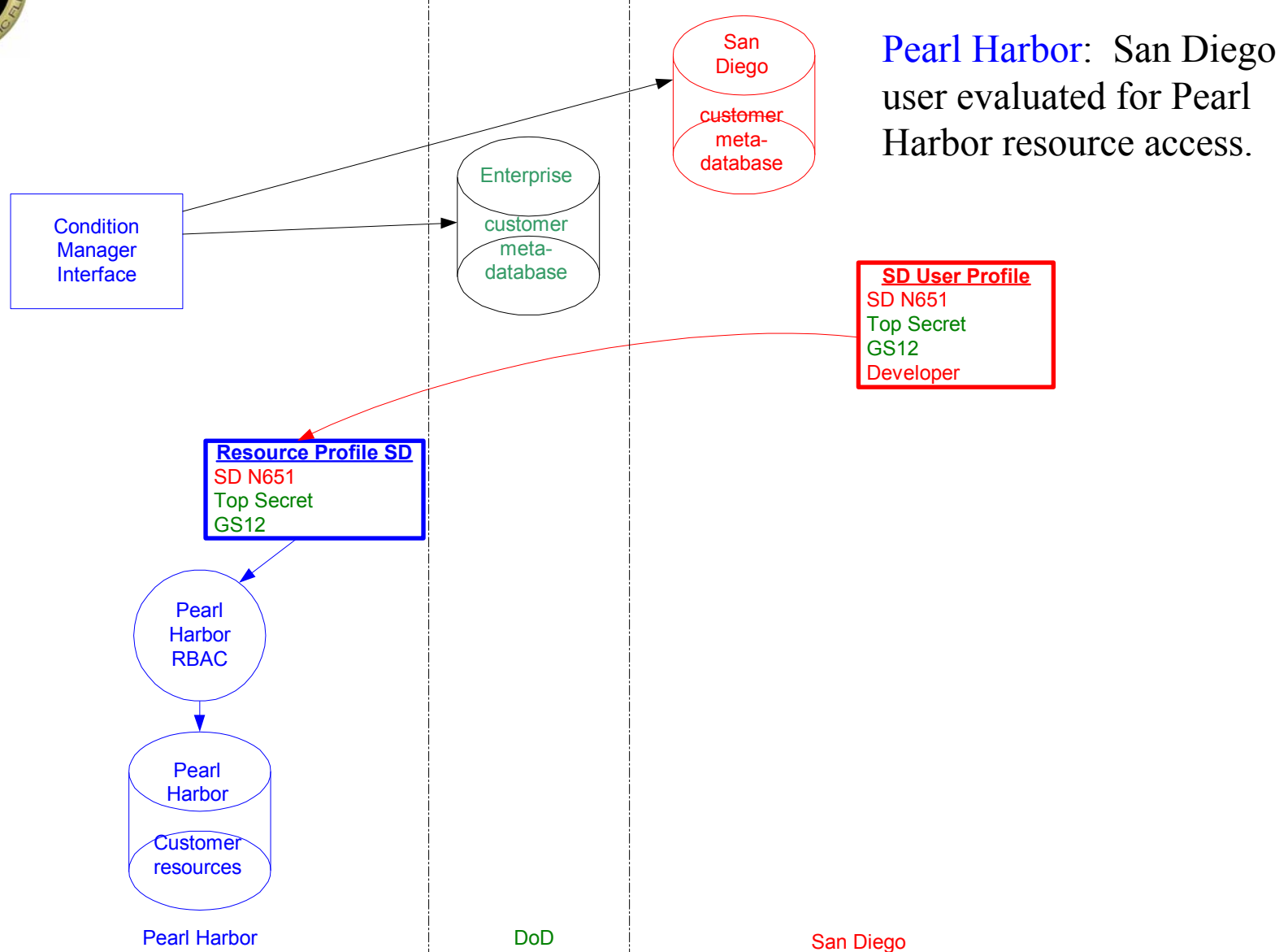


SEAC RBAC - Interoperability



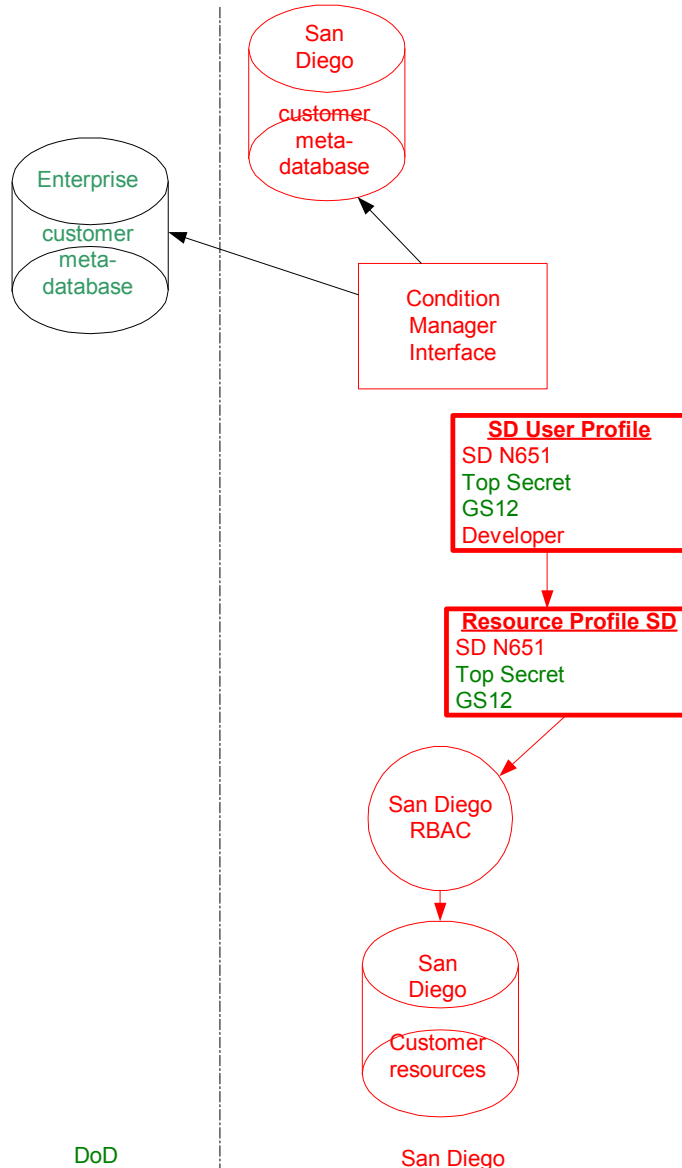


SEAC RBAC - Interoperability





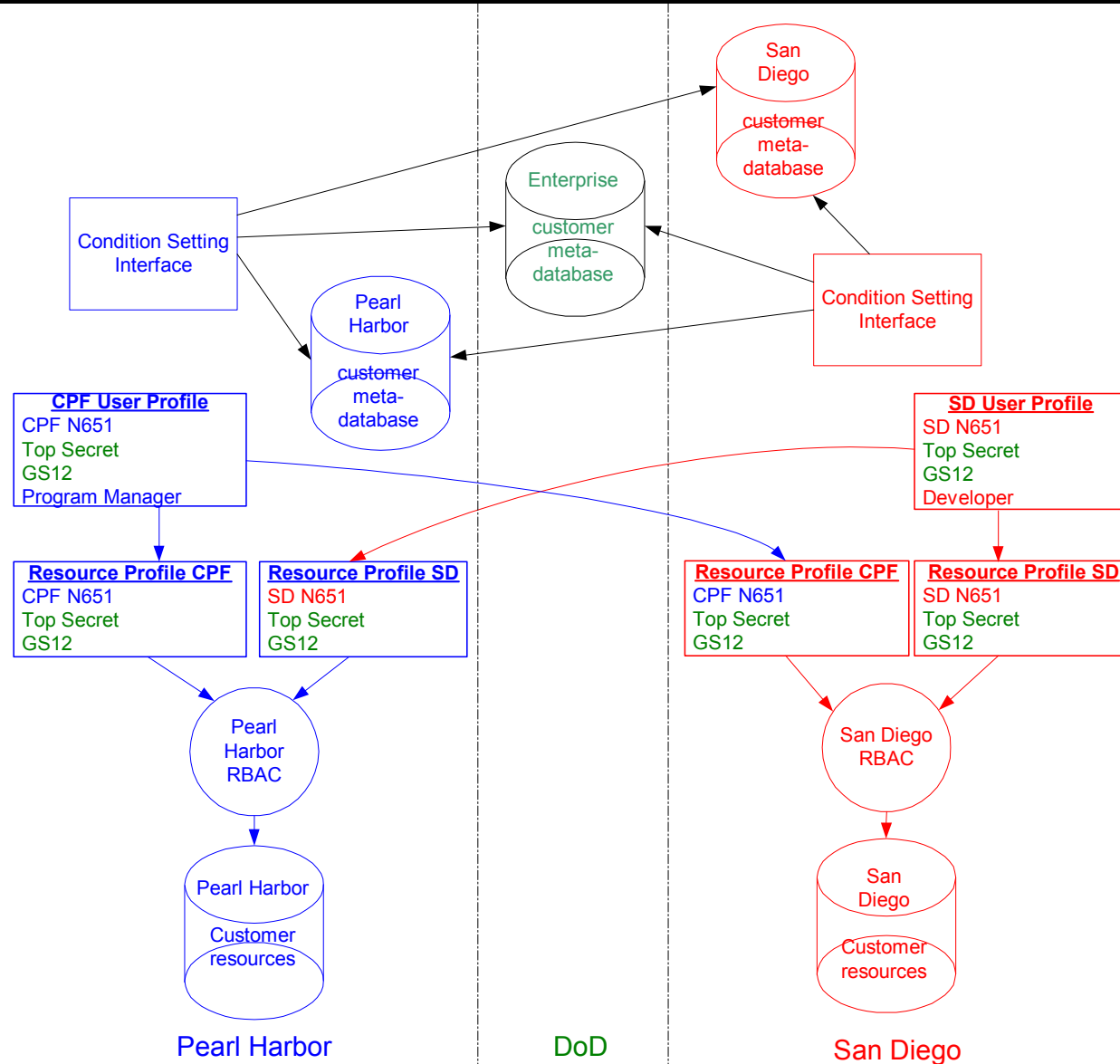
SEAC RBAC - Interoperability



San Diego: same user evaluated for San Diego resource access.



SEAC RBAC – Interoperability



The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

The information contained herein is considered U.S. Government Proprietary and may be related to one or more U.S. Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

SD 541, June 2004

SSC San Diego

San Diego, CA 92152-5001

Approved for public release; distribution is unlimited.